UNIVERSIDAD AMAZÓNICA DE PANDO

DIRECCIÓN DE POSTGRADO E INVESTIGACIÓN

TESIS PARA OPTAR EL GRADO ACADÉMICO DE MAGISTER EN INGENIERÍA INFORMÁTICA

Metodología para identificar vulnerabilidades y realizar análisis forense de los servidores de una organización

AUTOR: Lic. YARIA YORKA VILLCA PACA

TUTOR: M.Sc. Lic. JUAN RAMIRO VILLA

POTOSÍ– BOLIVIA

2012

DEDICATORIA

Este trabajo está dedicado a mi familia que es fuente de admiración, orgullo y respeto; quienes me apoyaron en todo momento para seguir estudiando y han seguido formándome con valores y principios.

AGRADECIMIENTOS

A Dios por el don de la vida y darme una familia que han sido los pilares más importantes en mi vida personal y profesional.

A mí amada madre Ancelma por darme su apoyo, fortaleza y guiarme por el camino del esfuerzo, a “Lizeth” mi hermana por siempre creer en mí. A “Hector” mi esposo por alentarme y comprenderme.

A mis docentes por transmitirme sus conocimientos y haber contribuido en mi formación profesional, en especial al tutor de la tesis M.Sc. Lic. Juan RamiroVilla por ayudarme en la realización y corrección de la misma, además de permitirme consultarle cada vez que necesite de su experiencia. También agradecer al M.Sc. Lic. Roberto Pérez cuya observación y oportunas sugerencias, contribuyo grandemente a perfeccionar este informe final.

Al técnico informático de la E.S.F.M. E.A. “Edson” por la información proporcionada para la elaboración de los resultados de la tesis.

A mis compañeros Lizeth, Lourdes, Iván y Daniel porque en su momento compartieron e intercambiaron sus conocimientos con mi persona.

A las prestigiosas universidades: Amazónica de Pando y Domingo Savio por darme la oportunidad de superarme en este sistema de educación.

Me hago responsable de todos los errores y agradecería mucho cualquier comentario acerca de este trabajo.

¡Gracias….!

ÍNDICE GENERAL

Página N°

RESUMEN……..……

INTRODUCCIÓN……..... 1

CAPÍTULO I. DISEÑO TEÓRICO METODOLÓGICO DE LA IDENTIFICACIÓN DE VULNERABILIDADES Y ANÁLISIS FORENSE DE SERVIDORES

1.1. Diseño teórico……..... 5

1.1.1. ***Planteamiento del problema***……... 5

1.1.2. ***Problema científico***……...……..... 6

1.1.3. ***Objeto de estudio***…...…….. 6

1.1.4. ***Campo de acción***…...…….. 7

1.1.5. ***Idea a defender***…...……. 7

1.1.6. ***Tareas científicas***…..…….. 7

1.1.7. ***Justificación de la investigación***…… 8

1.2. Diseño metodológico……..... 9

1.2.1. ***Tipo de investigación***……..... 9

1.2.2. ***Métodos de investigación***…… 9

CAPÍTULO II. SUSTENTO TEÓRICO DE LA IDENTIFICACIÓN DE VULNERABILIDADES Y ANÁLISIS FORENSE DE SERVIDORES

2.1. Metodología……..... 12

2.1.1. ***Estándares y normas internacionales y nacionales***……... 13

2.1.1.1. *Metodología de ataque a los servidores*…… 14

2.1.1.2. *Metodología OSSTMM – Manual de la metodología abierta del testeo de seguridad*……...…… 15

2.1.1.3. *Guía IOCE – Guía de la organización internacional de evidencia informática*……. 16

2.1.1.4. *Norma NB ISO/IEC 27001 – Especificaciones para sistemas de gestión de seguridad de la información (SGSI)*……... 18

2.1.1.5. *Norma NB ISO/IEC 27002 – Código de buenas prácticas para la gestión de seguridad de la información (GSI)*……..... 19

2.1.2. ***Procedimientos***……...……. 19
2.1.3. ***Herramientas***…….……..... 20
2.1.4. ***Tecnología del servidor***…….…… 21
2.2. Testeo de seguridad a servidores…….**.....** 22
2.2.1. ***Vulnerabilidades en los servidores***……..... 24
2.2.2. ***Acceso a los servidores***…… 24
2.2.3. ***Amenazas al servidor***…….. 25
2.2.4. ***Procedimiento de identificación de vulnerabilidades en los servidores***…… 27
2.2.4.1. *Identificación de vulnerabilidades*……..... 28
2.2.4.2. *Análisis y Corrección de vulnerabilidades*……..…..... 29
2.2.4.3. *Documentación de vulnerabilidades*……...…….. 30
2.3. Recuperación de evidencia de los servidores…….. 31
2.3.1. ***Análisis forense a servidores……..***……. 31
2.3.2. ***Procedimiento para realizar análisis forense a servidores***…… 32
2.3.2.1. *Identificación de evidencia*……..... 32
2.3.2.2. *Preservación de evidencia*…..……... 33
2.3.2.3. *Análisis de evidencia*……..…..... 34
2.3.2.4. *Documentación y presentación de las pruebas*……..... 35

CAPITULO III. METODOLOGÍA PARA IDENTIFICAR VULNERABILIDADES Y REALIZAR ANÁLISIS FORENSE DE SERVIDORES

3.1. Metodología de identificación de vulnerabilidades y análisis forense…..……..... 36
3.2. Metodología para la identificación de vulnerabilidades……..... 37
3.2.1. ***Prevención de vulnerabilidades***……...……..……. 39
3.2.1.1. *Evaluación de riesgos*…….…..... 39
3.2.1.2. *Gestión de vulnerabilidades*……..…..…….. 43
3.2.2. ***Identificación de vulnerabilidades***……...…….. 44
3.3.2.1. *Planificación de vulnerabilidades*……..…… 44
3.3.2.2. *Identificación de vulnerabilidades planificadas*……. 46
3.3.2.3. A*nálisis de vulnerabilidades*……..…… 47
3.3.2.4. *Búsqueda y verificación de vulnerabilidades reales*……..…… 48
3.2.3. **C*orrección de vulnerabilidades***……..... 49

3.3.3.1. *Búsqueda de correctivos*…… 50
3.3.3.2. *Informe final y presentación de la información*…… 50
3.3. Metodología para el análisis forense…… 51
3.3.1. ***Identificación de la evidencia***…… 53
3.3.1.1. *Solicitud forense*…… 54
3.3.1.2. *Asegurar la escena*…… 55
3.3.1.3. *Identificar las evidencias*…… 55
3.3.2. ***Preservación de la evidencia***…… 58
3.3.2.1. *Copias de la evidencia*…… 58
3.3.2.2. *Cadena de custodia*…… 59
3.3.3. ***Análisis de la evidencia***…… 60
3.3.3.1. *Preparación para el análisis*…… 61
3.3.3.2. *Reconstrucción de la secuencia temporal del ataque*…… 61
3.3.3.3. *Determinación de cómo se realizó el ataque*…… 62
3.3.3.4. *Identificación del atacante*…… 63
3.3.3.5. *Perfil del atacante*…… 63
3.3.3.6. *Evaluación del impacto causado al sistema*…… 63
3.3.4. ***Documentación y presentación de pruebas***…… 64
3.3.4.1 *Informe técnico*…… 64
3.3.4.2 *Informe ejecutivo*…… 65

CAPÍTULO IV. RESULTADOS DE LA APLICACIÓN DE LA METODOLOGÍA PROPUESTA

4.1. E.S.F.M. "E.A."…… 66
4.1.1. ***Diagnostico de la situación actual***…… 67
4.1.2. ***Justificativo del trabajo en la E.S.F.M. "E.A."***…… 68
4.1.3. ***Entorno de red y análisis de los servidores***…… 69
4.2. Metodología de identificación de vulnerabilidades…… 70
4.2.1. ***Prevención de vulnerabilidades***…… 71
4.2.1.1. *Evaluación de riesgos*…… 71
4.2.1.2. *Gestión de vulnerabilidades*…… 73
4.2.2. ***Identificación de vulnerabilidades***…… 74

4.2.2.1. *Planificación de vulnerabilidades*……..……..... 74
4.2.2.2. *Identificación de vulnerabilidades planificadas*……..... 76
4.2.2.3. A*nálisis de vulnerabilidades*…….…… 77
4.2.2.4. *Búsqueda y verificación de vulnerabilidades reales*……..... 78
4.2.3. C*orrección de vulnerabilidades*…….... 79
4.2.3.1. *Búsqueda de correctivos*……..... 79
4.2.3.2. *Informe final y presentación de la información*…… 79
4.3. Metodología de análisis forense…… 80
4.3.1. *Identificación de la evidencia*…….. 80
4.3.1.1. *Solicitud forense*……...……..... 80
4.3.1.2. *Asegurar la escena.*……...……...……... 81
4.3.1.3. *Identificar las evidencias*…….....…… 82
4.3.2. *Preservación de la evidencia*……... 83
4.3.2.1. *Copias de la evidencia*……... 83
4.3.2.2. *Cadena de custodia*……..... 84
4.3.3. *Análisis de la evidencia*…… 84
4.3.3.1. *Preparación para el análisis*……...…….. 84
4.3.3.2. *Reconstrucción de la secuencia temporal del ataque*……..... 85
4.3.3.3. *Determinación de cómo se realizó el ataque*…….....…….... 87
4.3.3.4. *Identificación del atacante*…...……..... 88
4.3.3.5. *Perfil del atacante*……...……... 88
4.3.3.6. *Evaluación del impacto causado al sistema*……...……... 89
4.3.4. *Documentación y presentación de pruebas*…… 89
4.4. Viabilidad de la metodología propuesta mediante el criterio de expertos…… 89
4.4.1. *Procesamiento de las encuestas a través del método Delphy*…… 90
4.4.2. *Análisis a los resultados del criterio de expertos*……..... 90
CONCLUSIONES…….. 91
RECOMENDACIONES……. 92
BIBLIOGRAFÍA……...…….…… 93
REFERENCIAS BIBLIOGRAFICAS…… 96
ANEXOS……...…….…….. 1

ÍNDICE DE CUADROS

Cuadro N°		Página N°
2.1	Herramientas para la identificación de vulnerabilidades y análisis forense……....	21
2.2	Puertos usados por aplicaciones en los servidores……....	22
3.1	Determinación de riesgo del servidor……...……...	40
3.2	Determinación de la severidad de pérdida de los riesgos…….....	40
3.3	Formulario de registro de amenazas……..….....	42
3.4	Formulario de registro de gestión de vulnerabilidades……..……..	43
3.5	Formulario de herramientas utilizadas en la identificación de vulnerabilidades…….	43
3.6	Formulario de estructura de red…….....	45
3.7	Formulario de registro de servidores…….…….....	45
3.8	Formulario de registro de vulnerabilidades internas……..….....	46
3.9	Formulario de registro de vulnerabilidades externas…….....	47
3.10	Formulario de registro de análisis de vulnerabilidades…….....	48
3.11	Formulario de registro de búsqueda y verificación de vulnerabilidades reales.....	49
3.12	Formulario de registro de la corrección de vulnerabilidades…..…….....	50
3.13	Formulario de informe final de vulnerabilidades encontradas en el servidor…….	51
3.14	Formulario de solicitud forense…….....	54
3.15	Formulario de rotulo de evidencias……...…….....	55
3.16	Formulario de daños producidos y recursos afectados……..….....	57
3.17	Formulario de criticidad de los daños…….....	57
3.18	Formulario de herramientas utilizadas en el análisis forense……...……...	58
3.19	Formulario de control de copias de evidencias…….	59
3.20	Formulario de cadena de custodia…….	60
3.21	Formulario del contenido de un informe técnico…….....	65
3.22	Formulario del contenido de un informe ejecutivo…….....	65
4.1	Determinación de riesgo del servidor-2…….....	71
4.2	Determinación de la severidad de pérdida de riesgos de los servidores atacados……	72
4.3	Formulario de registro de amenazas del servidor-2…….....	72

4.4 Formulario de registro de gestión de vulnerabilidades del servidor-2…… 73
4.5 Formulario de herramientas utilizadas en la identificación de vulnerabilidades del servidor-2…….……..……..…….. 74
4.6 Formulario de estructura de red con respecto al servidor-2…… 75
4.7 Formulario de registro del servidor-2…….…..... 76
4.8 Formulario de registro de vulnerabilidades internas del servidor-2……..... 77
4.9 Formulario de registro de análisis de vulnerabilidades del servidor-2…… 78
4.10 Formulario de registro de búsqueda y verificación de vulnerabilidades reales del servidor-2…….……..... 78
4.11 Formulario de registro de la corrección de vulnerabilidades del servidor-2…..... 79
4.12 Formulario de solicitud forense del servidor-2……..…….....**.....** 80
4.13 Formulario de rotulo de evidencias del servidor-2…….....**.....** 81
4.14 Formulario de daños producidos y recursos afectados al servidor-2……..….....**.....** 82
4.15 Formulario de criticidad de los daños producidos al servidor-2…..…… 82
4.16 Formulario de herramientas utilizadas en el análisis forense del servidor-2…..... 83
4.17 Formulario de control de copias de evidencias del servidor-2……..…….....**.....** 84
4.18 Formulario de cadena de custodia del servidor-2…… 84

ÍNDICE DE GRÁFICOS

Gráfico N° **Página N°**

2.1 Mapa de seguridad OSSTMM……..... 16

2.2 Fases metodología forense según IOCE……..... 17

2.3 Circulo de Deming……..... 19

3.1 Metodología de identificación de vulnerabilidades y análisis forense…… 37

3.2 Proceso de identificación de vulnerabilidades……...……. 38

3.3 Fase I: Prevención de vulnerabilidades……... 38

3.4 Fase II: Identificación de vulnerabilidades……..... 39

3.5 Fase III: Corrección de vulnerabilidades……..... 39

3.6 Proceso de análisis forense…….…….... 52

3.7 Fase I: Identificación de la evidencia……..... 52

3.8 Fase II: Preservación de la evidencia……..... 53

3.9 Fase III: Análisis de la evidencia……. 53

3.10 Fase IV: Documentación y presentación…….....**.....** 53

4.1 Arquitectura de red con respecto al servidor atacado…….....**.....** 69

4.2 Escaneo de puertos abiertos del servidor-2 con TCPView…….....**.....** 77

4.3 Imagen del servidor-2 movido a la herramienta Volatility…….....**.....** 85

4.4 Sistema operativo del servidor-2 obtenido a partir de la imagen……..... 86

4.5 Resumen de procesos ejecutados del servidor-2 obtenido a partir de la imagen……. 86

4.6 Conexiones de puertos abiertos del servidor-2 obtenido a partir de la imagen….**.....** 88

ÍNDICE DE ANEXOS

Anexo N°		Página N°
1	Variables de la idea a defender…….....	1
2	Lista de módulos del mapa de seguridad de la metodología OSSTMM…….	3
3	Fases metodología forense según IOCE……..	5
4	Fases del SGSI determinado por NB ISO/IEC 27001…….	6
5	Dominios (11), objetivos de control (39) y controles (133) de NB ISO/IEC 27002…….....	7
6	Determinación del tamaño de la muestra…….....	8
7	Encuesta (dirigido al administrador del servidor, directores y personal administrativo)……...	9
8	Guía de entrevista (dirigido al administrador del servidor)…….....	12
9	Guía de observación (dirigido al administrador del servidor, directores y personal administrativo)……...	13
10	Análisis e interpretación a los resultados de la encuesta…….	15
11	Encuesta a expertos (dirigido a profesionales especialistas)…….....	24
12	Resumen de las valoraciones de viabilidad…….	26

RESUMEN

El desconocimiento y la falta de aplicación de métodos actuales de seguridad en equipos servidores permiten actividades criminales informáticas que a falta de leyes bolivianas y políticas organizacionales no son sancionadas, ocasionando en el peor de los casos: accesos no autorizados con perdida de datos y archivos, desconfiguración de sistemas y daño a los dispositivos. Es por ello que en este trabajo se investigó: ¿Cómo contribuir al testeo de seguridad y recuperación de evidencia de los servidores de una organización para identificar vulnerabilidades y realizar análisis forense?. Basada en una investigación Bibliográfica-Documental de teorías y leyes afines se dio solución con la "Elaboración de una metodología y su aplicación práctica" a través de una Investigación Descriptiva aplicando métodos de investigación teóricos en el desarrollo de los capítulos y métodos empíricos mediante la investigación de campo con sus respectivas técnicas (entrevista, encuesta y observación) que permitieron identificar factores utilizados por los administradores para dar seguridad a los equipos servidores de red. Con la metodología propuesta se concluye que es inevitable la necesidad de buscar amenazas, evidencias y causas cuando el servidor de una organización es comprometido en un crimen informático, su aplicación permite determinar las causas y dar solución garantizando la seguridad y satisfacción de los usuarios finales en el manejo de información del servidor.

Palabras clave: metodología, identificación de vulnerabilidades, análisis forense, servidores, OSSTMM, Guía IOCE, ISO/IEC 27001, ISO/IEC 27002

INTRODUCCIÓN

La informática como ciencia del tratamiento automático de la información con su tecnología y métodos facilita modernizar la forma de trabajo y comunicación de cualquier actividad mediante las redes de computadoras para compartir datos, sistemas software, archivos, programas y dispositivos físicos. El componente principal en una red de computadoras es el servidor de páginas web, correo electrónico, bases de datos, archivos y/o impresoras, por lo que es imprescindible garantizar su seguridad para evitar incidentes y suspensión de servicios.

Centrando el tema de seguridad a servidores de red de una organización (instituciones, empresas, cooperativas, otros) no existen sistemas completamente seguros. A medida que se crean nuevas técnicas para la transmisión de la información aparecen nuevas amenazas; como los intrusos (hackers y usuarios) que en mayor cantidad son usuarios internos ya sea consciente o inconscientemente. Estos intrusos son los que idean formas de acceso al servidor mediante la red u otro medio sin ser autorizados y/o detectados para mover algún archivo de directorio, inyectar virus, ocasionar un desastre mayúsculo como el borrar toda la información, robar información, desconfigurar los sistemas y otros; todo por motivos de curiosidad, sabotaje, beneficio, desprestigio, protesta o venganza.

Los accesos al servidor ocurren generalmente por que los administradores desconocen o no aplican métodos, normas, guías y/o políticas de seguridad. Siendo que: no activan las características avanzadas de seguridad disponibles, no aplican de manera sistemática los parches disponibles, no conocen donde se almacena la información sensible, también la complejidad e interconectado de la red hace que la seguridad sea exigente y especializada, incluso para muchos la seguridad no es prioridad si no se tiene información confidencial, además múltiples conexiones desde las aplicaciones hace menos sencillo el seguimiento de amenazas y vulnerabilidades.

Por tanto, es indispensable aplicar seguridad informática en los servidores y crear conciencia en los usuarios a fin de interiorizar las implicancias que esto significa.

Para dar seguridad a los servidores de red es muy importante seguir metódicamente una metodología, guía o norma para ejecutar la identificación de vulnerabilidades y análisis forense. Con el análisis e identificación de vulnerabilidades, se examina la robustez y seguridad de cada uno de los sistemas y dispositivos ante ataques, se obtiene la información necesaria para analizar cuáles son las contramedidas que se pueden aplicar con el fin de minimizar el impacto de un ataque. Mientras que la informática forense permite la solución de conflictos tecnológicos relacionados con seguridad informática y protección de datos. Gracias a esta disciplina, las organizaciones obtienen una respuesta a problemas de privacidad, competencia desleal, fraude, robo de información confidencial y/o espionaje industrial surgidos a través del uso indebido de las tecnologías de la información, porque mediante sus procedimientos se identifican, aseguran, extraen, analizan y presentan pruebas generadas y guardadas electrónicamente para ser aceptadas en un proceso legal o interno disciplinario.

Hoy en día, se tienen metodologías, guías y normas de seguridad que en esencia son bien intencionadas, pero la constante innovación tecnológica hace que cada vez sea necesaria la aplicación de nuevas metodologías adaptadas a los nuevos tiempos, porque las más modernas responden a problemas y necesidades más actuales.

Actualmente en Bolivia se tiene en proyecto: 1) la ley de informática forense y seguridad de software, 2) el convenio que se está negociando con diferentes instituciones para crear listas oficiales de peritos informáticos. También a lo largo de las ciudades capitales se lleva eventos de capacitación y entrenamiento a funcionarios de varias instituciones: Banco Mercantil, Entel, FELCC, FELCN, Viceministerio anticorrupción y otros; donde se combina el tema de seguridad, auditoria de sistemas con el derecho informático y la informática forense. En cuanto a la búsqueda de vulnerabilidades y hacer análisis forense en servidores de red de una organización, la mayoría de las veces resulta ser desconocido, no se sabe por dónde comenzar, que investigar o que preguntar, por lo que el personal responsable suele aplicar parches superficiales instalando programas en los equipos o no se preocupan mucho de la seguridad, pero cuando llegan a tener problemas el tiempo que emplean es mucho mayor al que podría demorar si existiera alguna política o procedimiento para el uso correcto de los recursos informáticos.

Como consecuencia de lo mencionado anteriormente, el presente trabajo propone procedimientos y herramientas integradas en una metodología para identificar las vulnerabilidades y hacer análisis forense al servidor de una organización. Habiendo identificado los siguientes aspectos a tratar y que orientaron a lo largo de la investigación.

Problema: ¿Cómo contribuir al testeo de seguridad y recuperación de evidencia de los servidores de una organización para identificar vulnerabilidades y realizar análisis forense?

Objetivo General: Elaborar una metodología que contribuya al testeo de seguridad y recuperación de evidencia de los servidores de una organización para identificar vulnerabilidades y realizar análisis forense.

Objetivos específicos:

- Elaborar una metodología para identificar vulnerabilidades de los servidores de una organización, basado en la metodología OSSTMM, normas ISO/IEC 27001, ISO/IEC 27002 y herramientas estandarizadas.
- Elaborar una metodología para realizar análisis forense a servidores de una organización; basado en la guía IOCE, normas ISO/IEC 27001, ISO/IEC 27002 y herramientas estandarizadas.
- Aplicar la metodología propuesta a una organización educativa para su ejemplificación.

Idea a Defender: La aplicación de una metodología desarrollada para la identificación de vulnerabilidades y análisis forense, permitirá un eficiente testeo de seguridad y recuperación de evidencia de los servidores de una organización.

Con respecto a la metodología de la investigación; el presente trabajo responde a una investigación de tipo descriptivo (diseño transaccional-descriptivo) y de tipo pragmática, por estar orientada al conocimiento de la realidad con la metodología propuesta y por la utilización práctica de los conocimientos en una organización. Así mismo, basado en los objetivos y la idea a defender, se utilizarón los métodos teóricos, empíricos y estadístico matemático.

A nivel teórico se emplearon los métodos de análisis-síntesis, inductivo-deductivo, abstracto-concreto, histórico-lógico, modelación, recopilación bibliográfico-documental; todos de gran utilidad en el estudio de fuentes impresas de información, en el procesamiento de los fundamentos científicos y de las apreciaciones de los numerosos autores que tuvieron que ser consultados.

A nivel empírico se hizo uso de los métodos de la encuesta, entrevista y observación para planificar y diagnosticar la situación de una organización educativa, mostrar su situación actual con respecto a la administración de sus equipos servidores. Además, se utilizo la encuesta con el método de consulta a expertos para la planificación y valoración de la propuesta desarrollada.

A nivel estadístico matemático se utilizo el método estadístico para determinar la muestra poblacional tanto de la E.S.F.M. E.A. como de los profesionales expertos, en el procesamiento e interpretación de los resultados de las encuestas y valoración de viabilidad de la propuesta metodológica.

Por lo mencionado en los anteriores párrafos, la presente investigación se desarrolló en cuatro capítulos. El primer capítulo es el diseño teórico metodológico, presenta la problemática que originó la investigación de este trabajo, elementos fundamentales que se plantearon para orientar toda la investigación: problema científico, idea a defender y diseño metodológico. El segundo capítulo contiene el sustento teórico de la investigación basada en información relevante y necesaria al problema de investigación; es decir, conceptos y teorías importantes que permitieron asumir una o varias posiciones teóricas encaminadas a la solución del problema. El tercer capitulo que es el sustento empírico de la investigación, presenta la metodología propuesta, basado en la elección de criterios del marco teórico e información empírica, con lo que se da respuesta al problema planteado y verificar la idea a defender en la respectiva contrastación de lo real con lo científico. Finalmente, el cuarto capítulo denominado resultados, se describe el diagnostico realizado a la E.S.F.M. E.A. y se explica la aplicación de la metodología propuesta además de los resultados obtenidos, también contiene la validación del trabajo de investigación.

CAPITULO I

DISEÑO TEÓRICO METODOLÓGICO DE LA IDENTIFICACIÓN DE VULNERABILIDADES Y ANÁLISIS FORENSE DE SERVIDORES

El capítulo presenta explícitamente el problema, objeto y campo de acción que se ha identificado en relación con la identificación de vulnerabilidades y análisis forense, también contiene los métodos que facilitaron la solución del problema científico.

1.1. Diseño teórico.

1.1.1. Planteamiento del problema.

Las computadoras y sistemas informáticos en los últimos años han evolucionado bastante, su conexión en red con servicio de internet, se consideran piezas fundamentales en la sociedad moderna para el manejo de información (datos), son herramientas que favorecen el progreso de una organización (empresa, institución, cooperativa, otros). De ahí que una gran mayoría de las organizaciones tienen computadoras servidores para administrar usuarios, sistemas de información, páginas web, archivos, servicio de internet, correo electrónico, bases de datos con un gran volumen de información personal, dispositivos de hardware como impresoras, fotocopiadoras, entre otros.

Los equipos servidores son administrados por personal que muchas veces no aplica métodos o procedimientos de seguridad por desconocimiento, falta de actualización, recursos económicos, falta de herramientas, complejidad de la red, entre otros almacenamiento de información sensible; solo utilizan parches disponibles. A esto se agrega que en Bolivia se tiene desconocimiento y vacío de leyes con respecto a la seguridad informática.

Desafortunadamente los criminales han encontrado en la tecnología nuevas formas de cometer delitos de distintas índoles; han pasado de una dimensión física de evidencia como son las huellas digitales, ropa, cabellos y sangre a una dimensión digital o electrónica donde la evidencia solo existe digitalmente, como el caso de accesos no autorizados al servidor para

realizar hurto de información confidencial, fraude, desconfigurar sistemas, provocar perdida de datos y archivos, dañar dispositivos con programas maliciosos, inyectar virus, instalar programas espías, etc. Estos criminales muchas veces son hackers o usuarios que reciben servicios del servidor; acceden sin permiso por diferentes motivos: curiosidad, venganza, sabotaje y desprestigio, logrando ocasionar en el peor de los casos grandes pérdidas económicas a la organización.

Actualmente, existen métodos y herramientas que permiten dar seguridad a las computadoras, examinando la robustez y nivel de seguridad mediante testeo, resolver conflictos tecnológicos de seguridad al recuperar evidencias. Sin embargo, no se tienen métodos específicos de seguridad de servidores que indiquen cuando hacer, que hacer, que y porque el administrador o especialista forense debe utilizar.

Por lo mencionado, se definió como situación problemática:

Los administradores de servidores de una organización, ante ataques por programas o personas intrusas, tienen necesidad de dar seguridad informática mediante testeos al servidor para detectar y solucionar fallas existentes, también si corresponde, recuperar evidencia del servidor, investigando accesos o ataques con el fin de solucionar delitos informáticos.

1.1.2. Problema científico.

Realizado el diagnóstico de la situación del objeto y descrito la problemática que origino la investigación, se planteó el siguiente problema científico:

¿Cómo contribuir al testeo de seguridad y recuperación de evidencia de los servidores de una organización para identificar vulnerabilidades y realizar análisis forense?

1.1.3. Objeto de estudio

Se determino como objeto de estudio: Seguridad informática.

1.1.4. Campo de acción.

En relación al objeto de estudio se definió como campo de acción: Seguridad en los servidores de una organización para identificar vulnerabilidades y realizar análisis forense.

1.1.5. Idea a defender.

Para dar solución al problema planteado, basado en los objetivos, se tomo en cuenta la teoría de una hipótesis causal multivariada, misma que permitió formular como idea a defender:

La aplicación de una metodología desarrollada para la identificación de vulnerabilidades y análisis forense, permitirá un eficiente testeo de seguridad y recuperación de evidencia de los servidores de una organización.

En Anexo N° 1 se tienen las variables identificadas, definiciones conceptuales y operacionales de la idea a defender.

1.1.6. Tareas científicas.

Para resolver la presente investigación, basado en la idea a defender, se planteó las siguientes tareas científicas:

- Sistematizar y estudiar los principales fundamentos teóricos metodológicos relacionados con la seguridad informática para la identificación de vulnerabilidades y análisis forense de los servidores de una organización.
- Analizar métodos actuales de seguridad de los servidores de una organización para identificar vulnerabilidades y realizar análisis forense.
- Desarrollar componentes estructurales de una metodología para la identificación de vulnerabilidades y análisis forense que permita un eficiente testeo de seguridad y recuperación de evidencia de los servidores de una organización.
- Determinar el grado de viabilidad de la propuesta de una metodología para identificar vulnerabilidades y realizar análisis forense de los servidores de una organización.

1.1.7. Justificación de la investigación.

La realización de la presente tesis, queda justificada por los siguientes aportes alcanzados:

- Conveniencia. Tiene la finalidad de guiar y orientar metódicamente en la identificación de vulnerabilidades y análisis forense con respecto a servidores de una organización para detectar amenazas y mejorar la seguridad, además de recuperar evidencia con el propósito de esclarecer y contrarrestar la intrusión (qué y cómo ocurrió).
- Aporte teórico. Se integran elementos teóricos fundamentales en la creación de una metodología para identificar vulnerabilidades y realizar análisis forense en los servidores de una organización, lo que servirá de base teórica a futuras investigaciones, a los responsables de administrar servidores y especialistas forenses en la solución de sus problemas de seguridad. También la metodología en cada fase permite documentar información del servidor, constituyéndose como apoyo administrativo e incluso jurídico para responsables y directivos de una organización.
- Aporte Social. Responde a una necesidad manifestada por organizaciones mediante los administradores de servidores y sus usuarios, ante la intrusión y desconocimiento de métodos actuales de seguridad para la identificación de vulnerabilidades y realizar análisis forense. Además, los resultados de la aplicación práctica de la metodología propuesta a la E.S.F.M. E.A., permitió dar mayor seguridad al servidor para reducir pérdidas personales e institucionales (interrupción de trabajo continuo ocasionando horas extras, robo de información, desprestigio, entre otros).
- Significación Práctica. Se da con los resultados de la investigación, la metodología propuesta y su ejemplificación a una organización educativa (E.S.F.M. E.A.), al proporcionar información que sirve de base para orientar la utilización de la metodología y aplicarse a todo tipo de organizaciones (instituciones, empresas, etc.) que tienen problemas de seguridad en sus servidores, sin importar su sistema operativo, bases de datos o aplicativos (software, antivirus o aplicaciones web), además la elección de herramientas y métodos de seguridad propuestos no restringen el introducir otras por parte del personal responsable, queda abierta a una nueva tecnología y necesidad.

- Utilidad metodológica. Se propone una metodología que en sus fases permite generar información a ser analizada y registrada en formularios que pueden ser modificados a necesidad, con la finalidad de encaminarse hacia la solución del problema de seguridad del servidor. Además, el registro de los formularios sirve de base para posteriores análisis de problemas similares.

1.2. Diseño metodológico.

1.2.1. Tipo de investigación.

El tipo de investigación definido para realizar la tesis, responde al diseño de investigación descriptivo (transaccional-descriptivo), cuyo objeto es describir dos o más variables en un momento determinado llegando a la modelación metodológica. También se determinó realizar una investigación pragmática con la utilización práctica de los conocimientos científicos obtenidos de la metodología propuesta.

1.2.2. Métodos de investigación.

Con el fin de orientar la investigación, se hizo uso de los métodos teóricos, estadístico matemático y empíricos, en función al objeto de estudio, idea a defender, tareas científicas y los objetivos operativos de cada capitulo a desarrollar.

Del nivel teórico, que permitió interpretar conceptualmente los datos empíricos encontrados, asimilar teóricamente la realidad, realizar el respectivo análisis y comparación de teorías, lograr proponer y aplicar la metodología de identificación de vulnerabilidades y análisis forense. Se utilizaron los métodos:

- Análisis-Síntesis. En el respectivo análisis de las diversas teorías y determinar su utilidad para el planteamiento del problema e idea a defender, también permitió asumir una o varias posiciones teóricas comprimidas en una respuesta al problema (la propuesta), así como en la aplicación de la metodología propuesta.

- Inductivo-Deductivo. En la elección del tema de investigación, los objetivos, el desarrollo del marco teórico, la solución del problema y en la aplicación de la metodología propuesta.
- Abstracto-Concreto. En el análisis y descomposición de conceptos abstractos, para luego comprender y lograr un nuevo conocimiento concreto con la propuesta.
- Histórico-Lógico. En el desarrollo del objeto de investigación mediante el análisis concreto de evolución y funcionamiento teórico con respecto a la seguridad informática.
- Modelación. En el objeto de investigación, así como en el desarrollo de la metodología propuesta y su aplicación, mediante el análisis, determinación de componentes y relaciones entre ellos.
- Recopilación Bibliográfico-Documental. En la búsqueda de información relacionada al tema de estudio, problema, objetivos, idea a defender y en el desarrollo de los capítulos de la investigación.

Del nivel empírico, que permitió la recopilación de información normada y real de la organización sujeta de estudio, para comprobar de manera práctica la idea a defender en un cuarto capítulo, además de verificar el problema, realizar la respectiva medición de las variables y contribuir a la validación de la metodología propuesta. Se utilizaron los métodos**:**

- Encuesta. Realizado a toda la muestra poblacional de la E.S.F.M. E.A. (30 personas), mediante los cuestionarios para la captación de opiniones acerca de la investigación y diagnosticar la situación actual de la institución con respecto a los servidores.
- Entrevista. Realizado al encargado de administrar los equipos servidores de la E.S.F.M. E.A. mediante conversaciones de naturaleza profesional de manera formal e informal acerca de las funcionalidades y nivel de seguridad de los servidores. Los datos e información obtenida se registraron en un cuestionario.
- Observación. Realizado a toda la muestra poblacional de la E.S.F.M. E.A. (30 personas) de manera estructurada y no estructurada, con el fin de conocer el comportamiento del objeto de estudio. La primera se utilizó en la búsqueda de información mediante la acción de observar directamente el funcionamiento de la institución e identificar a los usuarios para conocer el tipo y flujo de información del servidor y hacer un examen crítico del mismo. La segunda, a través de los apuntes de aquello que en lo personal se consideró significativo

para posteriormente clasificar y utilizar los datos que requieren los objetivos de la investigación. La obtención de datos e información se registro en cuestionario.

- Consulta a expertos. Realizado a una muestra poblacional de 7 profesionales especialistas, mediante el cuestionario para la validación empírico subjetiva de la presente investigación; con la finalidad de conocer la evaluación de la validez teórica y la viabilidad de la metodología propuesta así como las recomendaciones para su perfeccionamiento en la puesta en práctica.

Del nivel estadístico matemático, que permitió obtener el muestreo poblacional de la E.S.F.M. E.A. y de los profesionales expertos, procesar cuantitativamente los datos obtenidos con los métodos empíricos, además de enriquecer los criterios de valoración cualitativa a las respuestas obtenidas con los cuestionarios. Se utilizo el método:

- Estadístico. Utilizado para determinar a partir de las poblaciones sujeta de estudio, el tamaño de muestra mediante el muestreo no-probabilístico de tipo "Muestreo de Selección Experta", habiendo obtenido para la institución educativa E.S.F.M. E.A. una muestra de 30 personas con la finalidad de recabar información y conocer la situación actual con respecto a sus equipos servidores. La otra muestra obtenida es de 7 profesionales especialistas seleccionados mediante la aplicación del criterio de idoneidad y voluntariedad, con el fin de conocer su valoración sobre la viabilidad de la metodología propuesta.

  También permitió interpretar los resultados de las encuestas realizadas al personal de la E.S.F.M. E.A. y profesionales especialistas, a través de cuadros y gráficos comparativos con el respectivo promedio de datos, destacando aquellos aspectos que son fundamentales de reconocer; es decir, dar un diagnostico valorativo de las dificultades que inciden en la seguridad del servidor con el fin de encaminarse a la solución del problema planteado.

CAPÍTULO II

SUSTENTO TEÓRICO DE LA IDENTIFICACIÓN DE VULNERABILIDADES Y ANÁLISIS FORENSE DE SERVIDORES

El capitulo contiene literatura actual de trabajos más sobresalientes respecto a metodologías, identificación de vulnerabilidades y análisis forense en equipos servidores, un análisis crítico y reflexivo argumentado por una explicación, experiencias y/o posición teórica asumida.

2.1. Metodología.

La palabra metodología proviene del griego meta "más allá", odos "camino" y logos "estudio", referido a los métodos de investigación que se siguen para alcanzar una gama de objetivos en una ciencia. Por tal motivo se entiende por metodología como una parte del proceso de investigación que permite hacer las cosas en forma organizada, clara y precisa desde un módulo inicial hasta completar un módulo final, facilitando el descubrimiento de conocimientos seguros y confiables para solucionar problemas.

En una metodología se detallan procedimientos, herramientas, técnicas, actividades y demás estrategias metodológicas requeridas para la investigación, también se indica el proceso a seguir en la recolección de la información, así como en la organización, sistematización y análisis de los datos. Es importante no restringir la creatividad introduciendo estándares excesivamente formales e inflexibles que afecten la calidad de las actividades, cada actividad tiene una relación con el inmediatamente anterior y con el inmediatamente posterior, cada sección tiene aspectos interrelacionados a otras actividades y algunos se interrelacionan con todas las otras secciones. Criterio considerado en el desarrollo de la metodología propuesta.

Las metodologías de identificación de vulnerabilidades y análisis forense a servidores que están basado en estándares y normas, como menciona Herzog (2010), permiten la separación entre recolección de datos, tests de verificación de y sobre los datos recolectados, análisis de datos y elaboración del informe final, sin importar el tamaño de la organización y tecnología.

2.1.1. Estándares y normas internacionales y nacionales.

La información es un activo que como otros activos es esencial para una organización, su seguridad se refiera a la preservación de la integridad, confidencialidad y disponibilidad. Muchas veces por el tamaño que tiene la organización, la tecnología informática y el personal a cargo de la administración del sistema, generan un vacío en la seguridad que debe tener la información contenida en los servidores de la red. Por otro lado se tiene a intrusos que aprovechan la falta de seguridad, hacen que los ataques nunca terminen, y por lo general sus objetivos son fraude, extorsión, robo de información, venganza, causar daño de prestigio, tener ingresos, ser vistos como los mejores o simplemente el desafío de penetrar a un sistema. Razones que hacen importante conocer la metodología que usan para perpetrar ataques a la seguridad informática, afectando la confidencialidad, integridad y disponibilidad de la información. En consecuencia la información necesita ser protegido de amenazas, por lo que es importante conocer con qué soluciones contamos para prevenir, detectar y reparar siniestros de este tipo. Para esto existe un conjunto importante de metodologías[1] y guías estandarizadas[2], normas[3], entre otros; cuyo objetivo es gestionar la seguridad de la información.

Entre las metodologías estandarizadas OSSTMM **(**Open Source Security Testing Methodology Manual) desarrollado por ISECOM (Institute for Security and Open Methodologies) es gratuita, de aplicación en materia de identificación de vulnerabilidades. Mientras que la Guía IOCE (International Organization on Computer Evidence) desarrollado por la organización internacional de prueba informática es una guía estandarizada gratuita, de aplicación en la gestión de la evidencia digital forense. Ambos son internacionalmente aceptados para la práctica de seguridad informática, comprenden una serie de objetivos de control y seguridad por lo que son modelos compatibles con las normas ISO/IEC de la serie 270xx. Razones por las que se utilizaron como referencia en la propuesta metodológica de la presente investigación con el objetivo de tener un enfoque de gestión de seguridad de la información con respecto a servidores y definir las fases con sus actividades y plantillas.

[1]Metodología estandarizada: conjunto de métodos científicos desarrollados en base a normas de organizaciones internacionales como ISO, además de estar certificada para su utilización.

[2]Guía estandarizada: conjunto de acciones desarrollados en el marco legal de un país por un grupo de profesionales especialistas en el área y reconocidos por el gobierno como institución para emitir guías.

[3]Norma: principio que se impone o se adopta para la correcta realización de una acción o el correcto desarrollo de una actividad. Una norma es certificable por las entidades correspondientes.

En lo referente a normas, la ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) son organizaciones no gubernamentales y forman el sistema especializado para la estandarización mundial, juntos participan en el campo de tecnologías de la información, preparan y publican normas con el objetivo de mostrar eficiencia en cuanto a calidad y mejoramiento de procesos. A semejanza de otras normas ISO/IEC, la serie 270xx (27000 a 27019 y 27030 a 27044) es un conjunto de estándares complementarios entre si, han sido desarrollados para sistemas de gestión de seguridad de la información (SGSI), es utilizable para cualquier tipo de organización, sus objetivos son:

- Establecer un marco metodológico para un SGSI.
- La adopción de controles proporcionales a los riesgos percibidos.
- La documentación de políticas, procedimientos, controles y tratamiento de riegos.
- Identificación y asignación de responsabilidades al nivel adecuado.
- Formalización, seguimiento y revisión de los controles y riesgos, de forma sistemática (periódica) y metodológica.
- Generación y preservación de evidencias.
- Tratamiento de los incidentes de seguridad.
- Revisión y mejora continúa del SGSI.
- Gestión de Riesgos.
- Uso de métricas para evaluar efectividad y eficiencia de controles y del propio SGSI (Pallas, 2009:7).

En Bolivia IBNORCA (Instituto Boliviano de Normalización y Calidad) aprobó el año 2007 una actualización de la norma ISO, entre ellas NB ISO/IEC 27001 y 27002. Por lo se utilizó como base estas normas que permitieron determinar, aplicar y evaluar los procesos y fases de la metodología propuesta.

2.1.1.1. Metodología de ataque a los servidores.

El método más común utilizado para perpetrar ataques a los servidores mediante la red, consiste en los siguientes pasos:

- Identificar. Realizan un networks scanners para hacer un mapa de la red identificando dominios, servidores, sistemas operativos, recogen información sin atacar y descubren los servidores activos, servidores de correo, nombres de empleados y rango de direcciones IP.
- Explorar. Hacen un ports scanners de las máquinas para detectar: puertos abiertos a fin de identificar posibles exposiciones o vulnerabilidades a explotar, servicios a la escucha, sistemas operativos y sistemas activos.
- Enumerar. Obtienen usuarios válidos o recursos compartidos mal protegidos.
- Acceso. Realizan un passwords crakers, detectan usuarios y passwords válidos con el fin de acceder a los servicios.
- Escalar privilegios. Obtienen el super usuario (usuario administrador) que permite realizar todas las operaciones posibles en el sitio y/o la red.
- Robar accesos. Buscan otros accesos válidos o rutas que permiten obtener información de la organización.
- Cubrir huellas. Buscan logs y borran todas las pistas de auditoría de tal manera que salgan sin dejar rastro.
- Crear entradas traseras. Crean cuentas de usuario y buscan los archivos deseados.

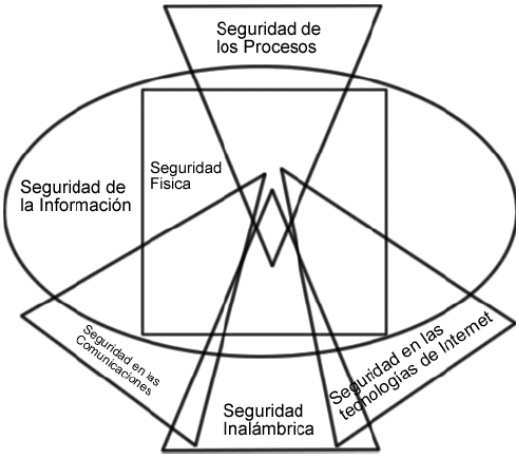
2.1.1.2. Metodología OSSTMM – Manual de la metodología abierta del testeo de seguridad.

OSSTMM es una metodología de código abierto para pruebas de seguridad y métrica de los sistemas y las redes que disponen una conexión a internet, es el estándar mas completo. Contiene un conjunto de reglas y lineamientos para cuando, que y cuales eventos son testeados, esta orientada a evaluar la seguridad de un sistema y realizar una auditoria de seguridad de los sistemas. Sin embargo, cubre solamente el testeo de seguridad externo, provee conceptos de ética profesional, pruebas integrales y lineamientos precisos a seguir en un test.

La metodología incluye un mapa de seguridad en espiral que comprende seis secciones, cada una con elementos de las otras secciones anteriores que habría que realizar para la ejecución de auditoria.

Gráfico N° 2.1

Mapa de seguridad OSSTMM



Fuente: Herzog (2010: 23)

Herzog (2010: 24-25) menciona la lista de módulos del mapa de seguridad, ver en Anexo Nº 2, que contienen planillas de datos de test de seguridad para describir los módulos y tareas que han sido testeados hasta su conclusión, cuales no han sido testeados hasta su conclusión y la justificación, cuales son los test no aplicables con su justificación, debe ser firmado por los testeadores acompañando todos los reportes finales. Las razones del uso de planillas de datos que sugiere la metodología son porque sirven de prueba del testeo de osstmm minucioso, responsabiliza a testeadores por el test, es una declaración precisa al cliente, brinda una apropiada visión general y suministra una lista de comprobación clara para el testeador.

2.1.1.3. Guía IOCE – Guía de la organización internacional de evidencia informática.

La guía IOCE es una guía para las mejores prácticas en el examen forense de tecnología digital, provee una serie de estándares, principios de calidad y aproximaciones para la detección, prevención, recuperación, exanimación y uso de la evidencia digital para fines forenses. Cubre los sistemas, procedimientos, personal, equipo y requerimientos de comodidad que se necesitan para todo el proceso forense de evidencia digital, desde examinar la escena del crimen hasta la presentación en la corte.

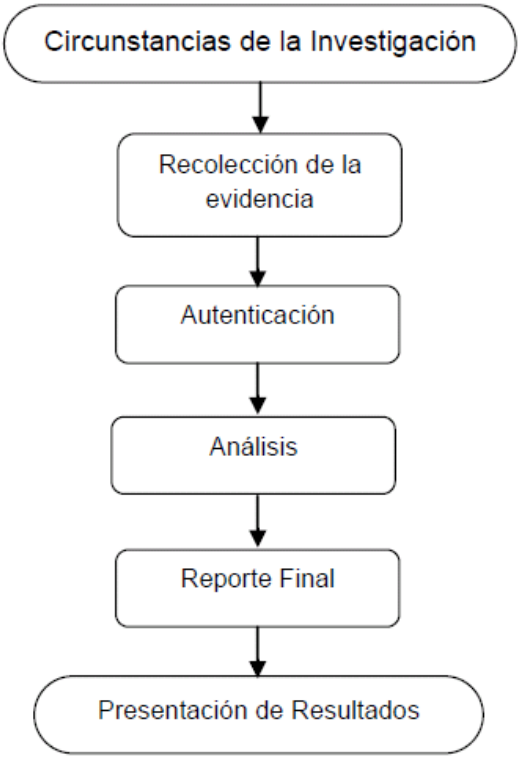
En 1999 la IOCE definió algunos principios internacionales para el manejo y recolección de la evidencia digital:

- Al recolectar la evidencia digital, las acciones tomadas no deben cambiar por ningún motivo la evidencia.
- Cuando una persona necesite acceder a la evidencia digital original, asegurarse de que sea un investigador forense competente.
- Toda la actividad relacionada con la recolección, acceso, almacenamiento o transferencia de evidencia digital, debe estar documentada, preservada y disponible para ser revisada.
- Un individuo es responsable por todas las acciones realizadas sobre la evidencia digital mientras se encuentre en su posesión.
- Cualquier agencia que sea responsable de recolectar, tener acceso, almacenar o transferir evidencia digital es responsable de cumplir con estos principios (cf. Lavin, 2010).

La metodología forense según la guía IOCE contiene un conjunto de actividades que pueden integrarse en 4 fases principales, ver anexo Nº 3 (cf. Almeida, 2011).

Gráfico N° 2.2

Fases metodología forense según IOCE



Fuente: Almeida (2011: 10)

2.1.1.4. Norma NB ISO/IEC 27001 - Especificaciones para sistemas de gestión de seguridad de la información (SGSI).

NB ISO/IEC 27001 sustituye a la BS 7799-2, es la norma principal de la serie 270xx de ISO/IEC, especifica requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI, a fin de permitir a una organización evaluar su riesgo e implementar controles apropiados para preservar la confidencialidad, integridad y disponibilidad de los activos de la información, además de ser certificable. En su anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI, no es obligatoria la implementación de todos los controles enumerados en dicho anexo. Sin embargo, la norma esta orientada a controles y no tanto a necesidades propias de la organización y no especifica un flujo de trabajo con procesos bien definidos.

Las especificaciones de la norma para SGSI son:

01. Alcance
02. Referencias sobre normativa
03. Términos y definiciones
04. Sistema de gestión de la seguridad de la información (SGSI)
05. Responsabilidad de la dirección
06. La auditoria interna
07. Revisión por la dirección
08. El proceso de mejora

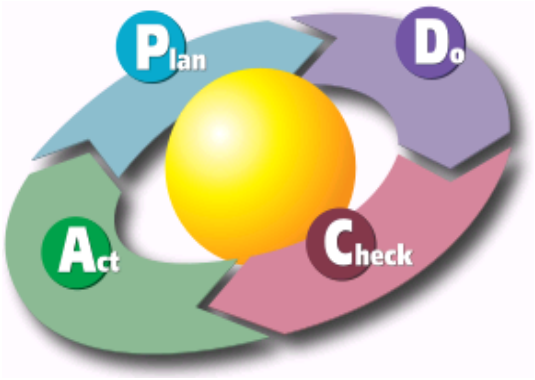
Para mantener la eficacia del SGSI los lineamientos metodológicos y requerimientos de la norma son propuestos bajo el enfoque metodológico del circulo de Deming[4] con cuatro fases (Plan-Do-Check-Act) que deben ser implementadas cíclicamente.

El anexo A de la norma comprende estas fases que contienen actividades, ver anexo Nº 4 (cf. Kosutic, 2012).

[4]Circulo de Deming: conocido ampliamente por sus siglas como ciclo PHVA (en español) o ciclo PDCA (Inglés), también denominado espiral de mejora continua de la calidad, es muy utilizado por los sistemas de gestión de calidad (SGC).

Gráfico N° 2.2

Circulo de Deming



Fuente: Pagina web http://es.wikipedia.org/wiki/C%C3%ADrculo_de_Deming

2.1.1.5. Norma NB ISO/IEC 27002 - Código de buenas practicas[5] para la gestión de seguridad de la información (GSI).

Es el nuevo nombre de ISO 17799:2005 mantiene intacto su contenido y su relación mediante el anexo A del estándar ISO 27001. Describe recomendaciones para realizar una gestión eficaz de la seguridad de la información, facilitando una base común que permite desarrollar normas de seguridad que proporcionen confianza dentro de las organizaciones. No es certificable. La norma es una guía de buenas prácticas que describe 39 objetivos de control y 133 controles agrupados en 11 dominios, ver en Anexo Nº 5 el listado propuesto por ISO (2012).

Los objetivos de control y controles existentes son para que una organización pueda escoger, es libre de agregar objetivos de control separados y controles existentes, de tal forma que puedan manejar las amenazas actuales o potenciales de seguridad de la información.

2.1.2. Procedimientos.

Procedimiento es un conjunto de métodos que se siguen para alcanzar los objetivos de una determinada investigación garantizando un enfoque consistente y repetitivo de las actividades.

[5]Buena práctica: son aquellas acciones que se caracterizan por haber logrado cumplir eficazmente las metas planteadas, y que luego de la evaluación de resultados, se ha concluido que proporcionan beneficios óptimos. No es certificable porque sólo se tiene como una buena alternativa por haber sido demostrado que ha funcionado.

Los procedimientos de identificación de vulnerabilidades y análisis forense en servidores son pasos que se siguen para ser validos ante instancias directivas o judiciales, cumplen con dos características esenciales, la primera es el método científico que permite demostrar que el resultado es repetible tantas veces sea necesario llegando al mismo resultado, la segunda es mantener la integridad desde el inicio hasta el final del proceso.

2.1.3. Herramientas.

Una herramienta es un programa que permite proteger, verificar y violar la seguridad de un equipo servidor u otro tipo de sistema, por lo que es recomendable tener una computadora que pueda soportar realizar adquisición, test y análisis. Existen diversas herramientas especializadas que pueden usarse como soporte a la aplicación del proceso de identificación de vulnerabilidades y análisis forense de equipos servidores, es posible encontrar desde las más sencillas que son gratuitas o económicas hasta muy sofistificados que incluyen software y dispositivo de hardware. En conclusión cada herramienta tiene ventajas y limitaciones, con cada una de ellas se puede realizar diferentes procesos, por lo que es importante contar con una gran variedad de herramientas para agilizar el trabajo de búsqueda de información, además de identificar datos que una herramienta en especial no puede detectar, haciendo la investigación más confiable y formal frente a entes directivos, judiciales y/o legales.

Las herramientas de software libre son de código abierto (Open Source), poseen una colección de herramientas en un solo software (toolkit) que pueden ser descargados libremente desde las páginas web de sus correspondientes autores o miembros del proyecto, cumplen similar funcionalidad a las herramientas que son comerciales. El sistema operativo Linux, tiene un entorno ideal que permite proveer de una gran variedad de herramientas que facilitan todas las etapas en la realización de un test y análisis exhaustivo.

Una herramienta completa incluye el siguiente kit de características técnicas:

- Herramientas para examinar procesos
- Herramientas para analizar el estado del sistema
- Herramientas para generar cadenas MD5

- Programas para generar imágenes bit a bit y poder analizarlas
- Scripts para la recolección de evidencias
- Herramientas para monitoreo y/o control de computadores
- Herramientas de marcado de documentos
- Herramientas de hardware (cf. Borghello, 2007)

Los responsables de administrar servidores deben tener en cuenta todos los factores mencionados anteriormente, además de conocer de la herramienta seleccionada de donde viene, como trabaja y haberla probado en un área restringida antes de usarla para conocer su rendimiento y confiabilidad de resultado, sin dejar de lado detalles normales como soporte, presupuesto y capacitación. En el siguiente cuadro se describe un resumen de herramientas.

Cuadro N° 2.1

Herramientas para la identificación de vulnerabilidades y análisis forense

Herramienta	Software Libre	Sistema Operativo	Descripción
Nessus	Si	Linux, Unix	Herramienta de evaluación de seguridad, es un escáner remoto que realiza más de 1200 pruebas y sugiere soluciones. Permite generar reportes en html, xml y ascii.
DSniff	Si	Linux, Unix, Windows	Poderosas herramientas de auditoría, pruebas de penetración de servidores y redes. Monitorean pasivamente en busca de datos (passwords, e-mail, arehivos, etc.), entre otros.
Traceroute/ping/ telnet/whois:	Si	Linux, Unix, Windows	Lo básico para ayudar en auditoría de seguridad.
Perl/Python	Si	Linux, Unix, Windows	Lenguaje de scripting de propósito general para múltiples plataformas (portable). Permite comprobar, arreglar sistemas, entre otros.
ISS Internet Scanner	No	Windows	Evaluación de vulnerabilidades a nivel de aplicación.
Volatility	Si	Linux, Windows	Conjunto de herramientas desarrolladas en Python para analizar capturas de memoria RAM, entre otros.

Fuente: Elaboración propia en base a página web (cf. Fyodor, 2012)

2.1.4. Tecnología del servidor.

En las redes de computadoras, los servidores son los que comparten sus recursos con otras computadoras y las proveen de servicios, esto hace que sea de mucho interés para los intrusos que intentan o acceden al servidor para robar información, alterar datos, desconfigurar los sistemas y ocasionar perdida de datos.

Los ordenadores para comunicarse en red entre si e intercambiar datos con sistemas operativos y hardware muy distintos, requieren de un medio, en el nivel físico esto se realiza a través de placas de redes y una conexión entre las mismas, a este lenguaje se llama protocolo.

Los servidores y computadoras en red tienen asignado una dirección IP (protocolo de internet) de 4 bytes (ej. 192.168.0.1). En un servidor para acceder desde el nivel de red al nivel de aplicaciones, no sirve simplemente indicar la dirección IP, se necesitan más especificaciones para que el host de destino pueda escoger la aplicación correcta. Sin embargo, sirve para etiquetar como principal sospechoso de un delito al usuario responsable. Actualmente existen miles de puertos $2^{16} = 65535$, de estos cuatro son más utilizados.

- Desde 0 hasta 1023 son conocidos y utilizados por aplicaciones de servidor.
- Desde 1024 hasta 49151 son registrados y asignados dinámicamente.
- Des 49152 hasta 65535 son puerto privados

Cuadro N° 2.2

Puertos usados por aplicaciones servidor

Puerto	Aplicación	Protocolo	Descripción
20	FTP-Data	TCP/UDP	Transferencia archivos
21	FTP	TCP	Control transferencia archivos
23	TELNET	TCP/UDP	Servicio remoto
25	SMTP	TCP/UDP	Envió de mails
43	Whois	TCP/UDP	
53	DNS	TCP/UDP	Servicio de nombre de dominios
70	Gopher	TCP/UDP	
80	WWW-HTTP	TCP/UDP	Word Wide Web

Fuente: (cf. Borghello, 2007)

2.2. Testeo de seguridad a servidores.

El testeo de seguridad es un test que se efectúa por sección a todo un sistema de computación. En equipos servidores consiste en realizar un test de servicios, puertos abiertos y otras vulnerabilidades conocidas, además de efectuar un análisis sobre ellos con el fin de proteger la

información contenida en las bases de datos y archivos. Este testeo puede ser manual al requerir que una persona ingrese datos durante el proceso y monitoreo de los resultados.

Para realizar testeo de vulnerabilidades a servidores es importante definir el modo correcto, se debe aplicar un test metódico de seguridad que se apoya en una combinación de creatividad, extensas bases de conocimiento sobre métodos más adecuados, cuestiones legales y regulaciones inherentes al área de una organización; todo para realizar un test exhaustivo, reducir la incidencia de muchos falsos supuestos y evitar resultados mediocres. Las preguntas a realizarse durante este proceso son:

- ¿Cómo acceder y en qué momento puedo provocar el máximo riesgo de seguridad?
- ¿Bajo qué circunstancias encuentro la mayor parte de las vulnerabilidades?
- ¿Cuándo estoy más propenso a aplicar confidencialidad, integridad y accesibilidad al test?

Un criterio a seguir para evitar actividades que no van con un test de seguridad de los servidores, es el testeo de vulnerabilidades para recolectar datos y obtener información con respecto a:

- Respuestas del Servidor de Nombres.
  - Examinar la información del registro de dominio en busca de servidores.
  - Encontrar el propietario del bloque de direcciones IP.
  - Examinar los servidores de nombres primario, secundario y del ISP en busca de subdominios.
  - Encontrar bloques de Ips como Ipv6, utilizados a través de consultas a los DNS.
- Pistas de la organización a analizar.
  - Inspeccionar los logs del servidor y los logs de intrusión en busca de eventos de los sistemas.
  - Inspeccionar mensajes de grupos de noticias y listas de distribución en busca de eventos de los sistemas.
- Filtración de información
  - Examinar el código fuente y scripts del servidor en busca de servidores de aplicación y enlaces internos.
  - Examinar las cabeceras de los correos electrónicos, los mensajes devueltos y los destinatarios de las alertas y eventos del sistema de los servidores.
  - Buscar información sobre la organización a analizar en los grupos de noticias.
  - Buscar en bases de datos dentro de la organización a analizar, referencias a hardware y software (cf. Herzog, 2010).

2.2.1. Vulnerabilidades en los servidores.

La vulnerabilidad debe entenderse como la carencia de recursos y capacidades de todo tipo para hacer frente a las amenazas o desastres; bajo esta denominación la vulnerabilidad de servidores es la debilidad o ausencia de controles adecuados en los sistemas, programas y otros que pueden desembocar en un problema de seguridad afectando la confidencialidad, disponibilidad e integridad de la información. Por lo general permite que un atacante pueda engañar a la aplicación esquivando los controles de acceso o ejecutando comandos en el sistema donde se aloja la aplicación.

2.2.2. Acceso a los servidores.

El acceso es el punto de entrada a un nivel de seguridad del servidor, esto puede incluir a una base de datos, página web, una conexión de red o cualquier cosa cuya ubicación soporte la definición de casi-público. Limitar el acceso significa negar todo excepto lo que este expresamente permitido por buenas prácticas.

El acceso a internet, se lo realiza mediante un proveedor quien asigna direcciones IP para configurar la red de computadoras; son los intrusos quienes para acceder al servidor averiguan sus direcciones y puertos, que en otros casos estos datos lo utilizan con el fin de acceder a servidores y equipos clientes de otras redes.

El control de acceso a los servidores se realiza, como menciona Bello (2011), para detectar actividades anómalas, normalmente este trabajo es realizado por programas a los que se les dan normativas de qué y cómo comparar, escanean archivos “log” con diferentes fechas, ante la detección de un desvío generan reportes informando el mismo.

Otro criterio a tener en cuenta es el mencionado por Herzog (2010), que el control de acceso a los servidores consiste en proteger:

- Servicios y acceso a Internet.
  - No usar acceso remoto no encriptado.

- No usar acceso remoto no autenticado.
- Las restricciones deniegan todo y permiten específicos.
- Monitorear y registrar todo.
- Descentralizar.
- Limitar la confianza entre sistemas.
- Poner en cuarentena las entradas y validarlas.
- Instalar únicamente las aplicaciones / servicios requeridos.

- Aplicaciones.
  - El uso de las características de seguridad debe ser una obligación.
  - Asegurar las justificaciones de la organización para todas las entradas y salidas en una aplicación.
  - Validar todas las entradas.
  - Limitar confianzas (a sistemas y usuarios).
  - Encriptar datos.
  - Encriptar los componentes.
  - Todas las acciones ocurren del lado del servidor.
  - Definir capas de seguridad.
  - Es mejor invisible - mostrar únicamente el servicio.
  - Accionar alarmas.

2.2.3. Amenazas al servidor.

Los abusos y ataques informáticos han surgido de diversas maneras y formas, estos son ocasionados por humanos o programas.

- Amenazas Humanas. Atentan contra la seguridad informática de una organización, suelen aprovechar ilícitamente las vulnerabilidades de los servidores para acceder a datos o programas. Realizan:

  - Manipulación de datos. Es una alteración o modificación de datos, ya sea suprimiendo, introduciendo datos nuevos y falsos, colocando datos en distinto momento o lugar. Este fraude representa el delito informático mas fácil de cometer y difícil de descubrir.
  - Manipulación de programas. Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos de informática. Consiste

en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o rutinas. Uno de los métodos utilizados es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

Las amenazas humanas, son atacantes externos que acceden remotamente al servidor e interceptan el tráfico de red o son empleados internos. Están clasificados como:

- Hackers. Se trata de personas con conocimientos en técnicas de programación, redes, internet y sistemas operativos; están siempre en continua búsqueda de información, viven para aprender y todo para ellos es un reto, no existen barreras y luchan por la difusión libre de información, distribución de software sin costo y globalización de la comunicación. Sus ataques suelen tener motivaciones de tipo ideológico (pacifistas, ecologistas, etc.) o simplemente un desafío intelectual.
- SciptKiddies. Se trata de jóvenes que con unos conocimientos aceptables en internet y programación emplean herramientas ya fabricadas por otros para realizar ataques.
- Profesionales. Son personas con conocimiento en lenguajes de programación, internet, sistemas operativos, redes y su equipamiento (routers, firewall, etc.). Suelen realizar ataques bajo encargo, por lo que su forma de trabajar implica una exhaustiva preparación del mismo, recopilan información posible sobre sus objetivos y realizan un tanteo con ataques en los que no modifican nada ni dejan huellas.
- Personal interno. Las amenazas a la seguridad de un sistema, provienen del propio sistema informático, son los mismos usuarios, rara vez es tomado en cuenta porque se supone que se tiene ámbito de confianza en la organización. Sus ataques suelen ser de tipo intencional, pero generalmente son accidentes por desconocimiento o inexistencia de normas básicas de seguridad.
- Expersonal interno. Se trata de personas descontentas con la organización porque han sido despedidos o renunciado, conocen a la perfección la estructura del sistema y tienen los conocimientos necesarios como para causar cualquier tipo de daño.

- Amenazas por programas. Los programas que son amenazas para el servidor están desarrollados por hackers o programadores para acceder con algún objetivo que por lo general no son buenas intenciones. Están clasificados como:

  - Malware. Son programas o partes de ellos que tienen código malicioso y causan efecto negativo en las computadoras. Ejemplo:
    - Virus. Programas autos replicantes que igual a un virus biológico se adjuntan a otro programa o archivo. El virus se ejecuta solamente cuando se ejecuta el programa o se abre el archivo infectado.
    - Gusanos. Son programas que una vez ejecutados se replican sin necesidad de la intervención humana, se propagan de ordenador en ordenador haciendo uso indebido de un servicio desprotegido atravesando la red de computadoras.
    - Troyanos. Programas que intentan mostrarse como algo útil o apetecible para que uno lo ejecute, una vez ejecutados intentan instalar un backdoor o rootkit, también suelen marcan un número telefónico de acceso a internet de alto coste.
    - Spyware. Programas que instalan clandestinamente código desde sitios de internet a los que se visita, una vez instalado busca en el ordenador información que considere de valor como un número de tarjeta de crédito.
    - Rootkits y backdoors; Son programas con códigos maliciosos que elaboran metodologías para permitir el acceso a un ordenador, van desde un programa escuchando en un puerto determinado hasta un programa que esconde sus procesos en memoria, modifica los archivos de registros y escucha en un puerto.

  - Exploit. Es un programa de prueba de concepto que puede estar escrito en código fuente para compilar, o en formato binario tipo .exe. Sirve para aprovechar o demostrar una vulnerabilidad en una aplicación.

2.2.4. Procedimiento de identificación de vulnerabilidades en los servidores.

Un procedimiento básico a seguir para la detección de vulnerabilidades en equipos servidores tiene cuatro fases: identificación, análisis, corrección y documentación de vulnerabilidades.

2.2.4.1. Identificación de vulnerabilidades.

Referido a los recursos que deben protegerse. Se identifican las vulnerabilidades del servidor con el fin de encontrar debilidades, errores de configuración y otros a nivel de:

- Seguridad física
  - Monitoreo ambiental
  - Control de acceso
  - Desastres naturales
  - Control de incendios
  - Inundaciones
- Seguridad en las conexiones a Internet.
  - VPN
  - Detección de intrusos
- Seguridad en Sistema Operativo
- Correo Electrónico
- Seguridad en las aplicaciones Críticas

El identificar vulnerabilidades en los servidores requiere de una búsqueda que consiste en comprobaciones automáticas de sistemas y aplicaciones, tal como lo menciona Herzog (2010):

- Integrar en las pruebas realizadas los escáneres, herramientas de hacking y exploits utilizados actualmente.
- Medir la organización objetivo utilizando herramientas de escaneo habituales.
- Enumerar Puertos:
  - Usar escaneos para enumerar puertos abiertos, cerrados o filtrados para aquellos puertos TCP
  - Usar escaneos TCP para enumerar puertos y servicios. Usar scaneos TCP full connect para escanear todos los puertos por encima del 1024.
  - Usar escaneos UDP para enumerar puertos abiertos o cerrados para los puertos UDP.
- Intentar determinar vulnerabilidades por tipo de aplicación y sistema.
  - Examinar las respuestas de los sistemas y aplicaciones para determinar el tipo de sistema operativo y su nivel de parcheado.
  - Relacionar la información recopilada con las respuestas de los sistemas para ajustar los resultados.
- Identificar servicios

- Relacionar cada puerto abierto con un servicio y protocolo.
- Identificar el nivel de parcheado del sistema a partir de su up-time

- Intentar ajustar vulnerabilidades a servicios.
- Intentar determinar el tipo de aplicación y servicio por vulnerabilidad.
- Realizar pruebas redundantes al menos con dos escáneres automáticos de vulnerabilidades.
- Identificar todas las vulnerabilidades relativas al sistema operativo y aplicaciones.
- Identificar todas las vulnerabilidades de sistemas parecidos o semejantes que podrían también afectar a los sistemas objetivos.
- Verificar todas las vulnerabilidades encontradas durante la fase de búsqueda de exploits con el objetivo de descartar falsos positivos y falsos negativos.
- Verificar todos los positivos (Se debe tener en cuenta el contrato firmado con la organización objetivo en el caso de estar intentando penetrar o si se puede llegar a provocar una denegación de servicio).

En esta etapa, la cantidad de tiempo otorgado para buscar y extraer información es dependiente del tamaño de la organización, el ámbito del proyecto y la longitud de tiempo planeado para el test. No obstante, mucho tiempo no siempre significa más información pero puede eventualmente llevar a partes claves del rompecabezas de la seguridad de los servidores.

2.2.4.2. Análisis y Corrección de vulnerabilidades.

El análisis de vulnerabilidades con respecto a servidores, puede ser determinado como lo menciona Geis y Silva (2009).

Preguntarse:

- ¿Cuánto daño podría ser causado?
- ¿Cuál es el impacto si se explota la vulnerabilidad?
- ¿Cuál es el valor de los sistemas afectados?
- ¿Cuál es el valor de los datos en esos sistemas?
- ¿Puede ser explota la vulnerabilidad en forma remota?
- ¿Qué nivel de habilidad y requisitos previos son necesarios por un atacante para explotar la vulnerabilidad?
- ¿Existe una solución para esta vulnerabilidad?
- ¿Cuál es la fuente de información que podemos utilizar para el análisis?

Responder:

- ¿Quién?, ¿Qué?, ¿Cuándo?, ¿Dónde?, ¿Por qué? y ¿Cómo?

Analizado las vulnerabilidades reales, corresponde corregir estableciendo las prioridades y orden de restablecimiento de los procesos que soportan a la organización para asegurar la pronta recuperación de las actividades normales y asegurar la continuidad de operaciones. Entre las posibles correcciones a realizar están:

- Básicas:
  - Instalación de un sistema operativo seguro (control de acceso y permisos)
  - Programa de antivirus actualizado
  - Cortafuegos personales de libre distribución (seguridad perimetral)
  - Programa detector de programas espías
  - Programa de mantenimiento del registro de Windows (si utiliza este sistema operativo)
  - Copias de seguridad
  - Normas de uso del correo seguro (Políticas de adjuntos, no previsualización, no HTML, SSH)
  - Normas de navegación segura (certificados, firma electrónica, SSL)
  - Actualizaciones de los parches de seguridad de las aplicaciones instaladas

- Avanzadas:
  - Sistemas de encriptación y autentificación *(GnuPGP*)
  - Detector de vulnerabilidades (detectores de fallos de seguridad: *network security scanner*)

2.2.4.3. Documentación de vulnerabilidades.

La documentación es un activo fundamental de la organización, tanto para completar el proceso de revisión, monitoreo y mejora del SGSI. Como tal, tiene atributos de confidencialidad, integridad y disponibilidad que son necesarios preservar. La cantidad y exactitud de documentación depende del tamaño y exigencias de seguridad de la organización. Una documentación detalla todos los hallazgos desconocidos, especifica claramente todos los estados de seguridad encontrados y no sólo las medidas de seguridad fallidas, contiene las soluciones prácticas orientadas a resolver los problemas de seguridad del servidor.

2.3. Recuperación de evidencia de los servidores.

La recuperación de evidencia consiste en averiguar lo ocurrido durante un delito o intrusión informática, busca dar respuesta a las interrogantes:

- ¿Quién lo realizó?
- ¿Qué hizo?
- ¿Cómo lo hizo?
- ¿Qué activos de información se vieron afectados?

Los objetivos por los que se realiza esta actividad son:

- Demanda legal.
- Investigación judicial.
- Parte del proceso de seguridad de la organización.
- Las evidencias pueden no ser válidas en un juicio pero ayudan a mejorar la seguridad.

Se requiere entonces de la aplicación de una metodología estandarizada que permita distorsionar lo menos posible la información con el objetivo de reconstruir todos los datos y/o eventos qué ocurrieron en el pasado.

2.3.1. Análisis forense a servidores.

El análisis forense es la aplicación de métodos con técnicas científicas y analíticas en investigaciones criminales, estas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos, valorar daños ocasionados y explicar las características técnicas del uso aplicado a los datos y bienes informáticos. López (2007) simplifica la definición de análisis forense a servidores, como el proceso de examinar dispositivos metódicamente (discos duros, disquetes, etc.) en busca de evidencias.

Existen dos modos de análisis forense que se aplican a los servidores:

- Análisis post-mortem. Se realiza cuando los daños han provocado la in operabilidad del sistema. Se examina con un equipo dedicado específicamente para fines forenses los discos duros, datos o cualquier tipo de información almacenada en memoria no volátil. Las herramientas de las que se puede disponer son aquellas destinadas al análisis de discos duros, archivos de logs, de firewall, etc.
- Análisis en caliente. Se lleva a cabo cuando un sistema presume que ha sufrido o está sufriendo un incidente de seguridad. En este tipo de casos se trata de analizar el contenido volátil, principalmente la memoria, se emplea un CD con las herramientas de respuesta ante incidentes y análisis forense compiladas de forma que no se realicen modificaciones en el sistema. Una vez hecho este tipo de análisis y confirmado el incidente se realiza el análisis post-mortem.

2.3.2. Procedimiento para realizar análisis forense a servidores.

Para la recuperación de evidencia, las metodologías en su generalidad implican cuatro fases:

- Se identifican posibles fuentes de evidencias.
- Se preservan estas evidencias.
- Se analizan (buscando respuestas a preguntas sobre un hecho).
- Se presentan las conclusiones y las evidencias que las sustentan López (2007).

2.3.2.1. Identificación de evidencia.

La evidencia digital es el conjunto de datos en forma binario, comprende ficheros, su contenido o referencia a estos que se encuentran en los soportes físicos o lógicos del sistema atacado. Son recolectados y analizados con herramientas y técnicas especiales que proporcionan como resultado dos tipos de evidencia digital:

- Constante: evidencia almacenada en un medio informático y que se mantiene preservada después de que la computadora sea apagada.

- Volátil: evidencia que se encuentra almacenada temporalmente como la memoria RAM o caché, que al interrumpir la alimentación eléctrica la evidencia se pierde. Este tipo de evidencia debe ser recuperada casi de inmediato guardando a ficheros para que se convierte en evidencia no volátil.

La identificación de evidencia se basa en la localización de las fuentes de información de una manera lógica, clara, exacta e inteligente, cuestionándose que información se requiere para poder realizar la investigación. Tanto López (2007) como Borghello (2007), ejemplifican las preguntas a plantearse y resolver durante el proceso de análisis forense:

- ¿Qué información se necesita?
- ¿Qué marca y características del hardware tiene el equipo o dispositivo a ser analizado?
- ¿Qué sistema operativo y aplicaciones se están utilizando en el equipo o dispositivo?
- ¿El equipo se encuentra encendido o apagado?
- ¿Cómo aprovechar la información presentada?
- ¿En qué orden ubico la información?
- ¿Acciones necesarias a seguir para el análisis forense?
- ¿Qué hizo denotar el incidente y qué acciones se tomaron?
- ¿A quién pertenece y quienes operan el equipo?

Esta fase inicia con la solicitud forense, donde se incluye toda la información necesaria para dar inicio al proceso de análisis, luego corresponde asegurar la escena del crimen para proceder con la identificación de la evidencia. El producto final es entregar un documento detallado con la información que permita definir un punto de inicio para la adquisición de datos y elaboración del documento final.

2.3.2.2. Preservación de evidencia.

Busca la integridad de la evidencia desde su obtención hasta la fase final. Se enfoca en resguardar los objetos que tengan valor como evidencia para que estos permanezcan de forma completa, clara y verificable. Para asegurar las evidencias es importante no generar cambios ante cualquier examen, se utilizan técnicas criptográficas como códigos de seguridad (función

hash, checksums), además realizar copias de la evidencia obtenida y generar una suma de comprobación de la integridad de cada copia utilizando funciones como MD5 o SHA1.

A esta fase se integra la cadena de custodia, que es el conjunto de pasos o procedimientos seguidos para preservar la prueba digital que servirá de evidencia en un proceso judicial, además se establecen responsabilidades y controles de cada una de las personas que manipulan la evidencia. López (2007) confirma que debe prepararse un documento en el que se registren los siguientes datos:

- Quién obtuvo la evidencia.
- Dónde y cuándo la evidencia fue obtenida.
- Quién protegió la evidencia.
- Quién ha tenido acceso a la evidencia.

2.3.2.3. Análisis de evidencia.

Se refiere a la interpretación de los datos obtenidos y su colocación en un formato lógico y útil. Proporciona evidencia que se busca y está en función de las habilidades del forense informático. Debe documentarse en todas sus partes y repetir el suceso cuantas veces sea necesario para demostrar que el resultado obtenido es el correcto.

Antes de realizar un análisis a las evidencias debe tenerse en cuenta la siguiente información:

- Sistema operativo afectado
- Inventario de software instalado en el servidor
- Tipo de hardware
- Accesorios y/o periféricos conectados al servidor
- Conexión y configuración a internet
- Parches y/o actualizaciones de software
- Políticas de seguridad implementadas
- Forma de almacenamiento de la información (cifrada o no)
- Personas con permiso de acceso al servidor

- Cuantos equipos en red reciben servicio del servidor
- Listar usuarios conectados local y remotamente.

El análisis se da por concluido cuando se descubre cómo se produjo el ataque, quién o quienes llevaron a cabo, bajo qué circunstancias se produjo, cuál era el objetivo, qué daños causaron.

2.3.2.4. Documentación y presentación de las pruebas.

La documentación es un activo mas, lo más importante de cada acción que se haya tomado en la investigación, con el fin de poder explicar el proceso de análisis ante cualquier instancia en cualquier momento. Describe lo sucedido en cada actividad para reducir las posibilidades de error y ser presentado legalmente a entidades investigadoras y judiciales, la misma debe ser:

- Entendible
- Constante y Reproducible
- Basada en un amplio periodo de tiempo
- Compatible con las leyes individuales, locales y con la legislación de la protección de datos
- Rigurosa
- Creíble
- Confiable
- Convincente

La aplicación de formularios ayuda a presentar una resolución del incidente mediante la presentación de informes técnico y ejecutivo (cf. Valdespino, 2009):

- Técnico. Contiene una explicación detallada del análisis efectuado, describe en profundidad la metodología, técnicas, hallazgos del equipo forense, conclusiones y recomendaciones. Este documento expone lo sucedido para personal especializado como forense informático.
- Ejecutivo. Contiene un resumen del análisis efectuado pero empleando una explicación no técnica, se exponen los hechos más destacables de lo ocurrido en el sistema analizado y se dan las recomendaciones, consta de tres a cinco páginas. Este informe expone lo sucedido para personal no especializado en sistemas informáticos departamento de recursos humanos, administración e incluso algunos directivos

CAPÍTULO III

METODOLOGÍA PARA IDENTIFICAR VULNERABILIDADES Y REALIZAR ANÁLISIS FORENSE DE SERVIDORES

El capítulo contiene la propuesta metodológica; su estructura conceptual, definición, representación gráfica y características. Todo desarrollado en base al objeto de estudio y objetivos de la investigación, con lo que se da solución al problema planteado y verificar la idea a defender.

3.1. Metodología de identificación de vulnerabilidades y análisis forense.

La metodología se presenta como una guía formal para identificar vulnerabilidades y realizar análisis forense de servidores, basado en los lineamientos y procesos de la metodología OSSTMM, guía IOCE, normas ISO/IEC 27001 y 27002. Su desarrollo y aplicación permitió dar cumplimiento a los objetivos planteados en la presente investigación; habiendo definido como objetivo general:

Elaborar una metodología que contribuya al testeo de seguridad y recuperación de evidencia de los servidores de una organización para identificar vulnerabilidades y realizar análisis forense.

Y objetivos específicos:

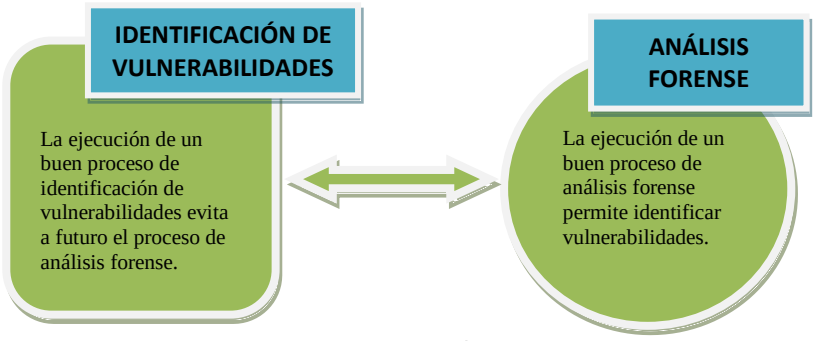
- Elaborar una metodología para identificar vulnerabilidades de los servidores de una organización, basado en la metodología OSSTMM, normas ISO/IEC 27001, ISO/IEC 27002 y herramientas estandarizadas.
- Elaborar una metodología para realizar análisis forense a servidores de una organización; basado en la guía IOCE, normas ISO/IEC 27001, ISO/IEC 27002 y herramientas estandarizadas.
- Aplicar la metodología propuesta a una organización educativa para su ejemplificación (desarrollado en Cap. IV).

Con la propuesta metodológica se integra dos procesos análogos: vulnerabilidades y análisis forense. Ambos se relacionan al permitir realizar un estudio adecuado de los sistemas, aplicaciones y servicios del servidor; que ante la posibilidad o sospecha de una violación de seguridad, se obtiene una evidencia valida en caso de incurrir en un acto legal. Además, se obtiene como resultado la mayor cantidad de información necesaria que responda a las particularidades de problemas de seguridad de la información en los servidores de una organización.

La estructura conceptual de la metodología es:

Gráfico Nº 3.1

Metodología de identificación de vulnerabilidades y análisis forense



Fuente: Elaboración Propia

3.2. Metodología para la identificación de vulnerabilidades.

La presente metodología permite identificar vulnerabilidades de servidores, su aplicación no restringe introducir otros procesos, subprocesos o algunas tareas, queda abierta a una interpretación en la que una nueva tecnología sea introducida.

El proceso es iterativo y repetitivo, cada una se realimenta de la fase anterior, comienza con la fase de prevención, prosigue con la fase de identificación y su ciclo termina con la fase de corrección de vulnerabilidades. Su proceso se enmarca en delimitar el problema previniendo e identificando las vulnerabilidades más simples y complejas de corregir, concluye con un listado de vulnerabilidades identificadas y corregidas. Lo más importante es que los diferentes tests sean evaluados y ejecutados donde sean aplicados hasta arribar a los resultados esperados

dentro de un período de tiempo determinado, solo así se habrá ejecutado el test en conformidad con la propuesta metodológica y orientar hacia un sistema seguro.

Gráfico Nº 3.2

Proceso de identificación de vulnerabilidades

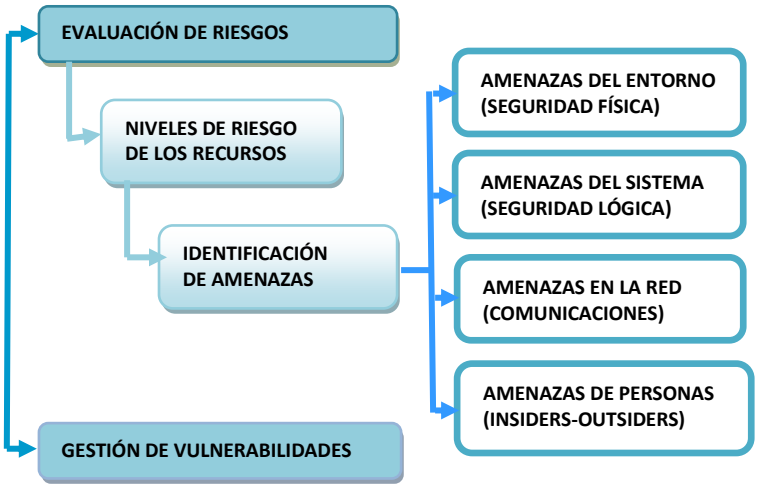


Fuente: Elaboración Propia

Cada fase contiene actividades, algunas dependen de la anterior actividad, tal como se muestra en los siguientes tres gráficos.

Gráfico Nº 3.3

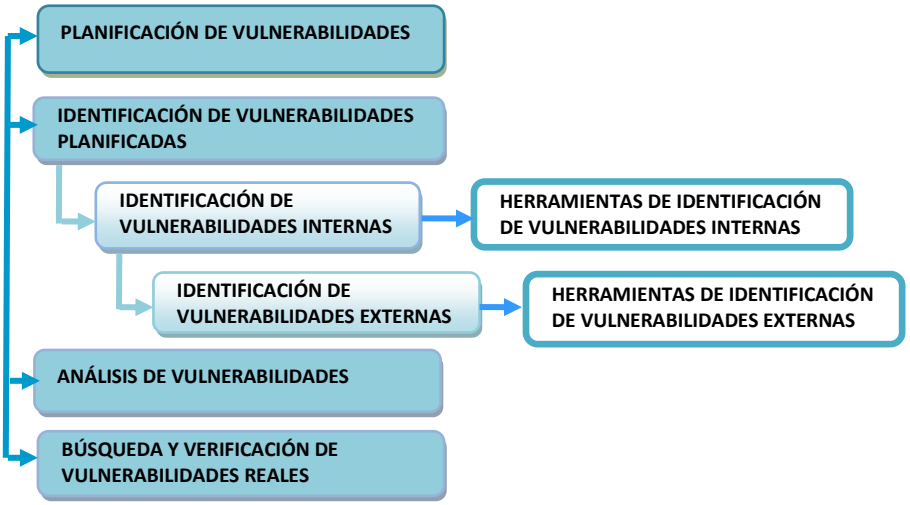
Fase I: Prevención de vulnerabilidades



Fuente: Elaboración Propia

Gráfico Nº 3.4

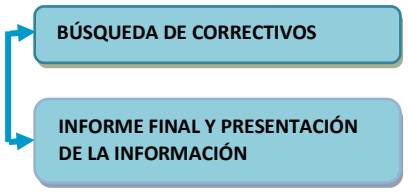
Fase II: Identificación de vulnerabilidades



Fuente: Elaboración Propia

Gráfico Nº 3.5

Fase III: Corrección de vulnerabilidades



Fuente: Elaboración Propia

3.2.1. Prevención de vulnerabilidades.

La prevención permite disminuir la aparición de vulnerabilidades al identificar las amenazas a la que se encuentran expuestos los servidores. Dependiendo que tan protegido esta el servidor de las vulnerabilidades, es necesario mejorar el proceso de seguridad e incrementar más tareas a realizarse por día(s). El prevenir, implica reconocer que recursos valen la pena proteger y entender que algunos son más importantes que otros.

3.2.1.1. Evaluación de riesgos.

Esta tarea consiste en predecir y adelantarse ante cualquier eventualidad que ponga en riesgo el perfecto funcionamiento de los servidores. Para esto:

- Tener en cuenta la probabilidad de que sucedan posibles problemas, priorizar.
- Conocer qué se quiere proteger, dónde y cómo identificar los recursos (hardware, software, información, personal, etc.) con que se cuenta y las amenazas a las que se está expuesto.

Para realizar esta tarea, obtener una lista de cada tipo de riesgo y determinar el factor de riesgo. Clasificar la lista por su nivel de importancia, de muy alto a muy bajo. Posteriormente tomar las medidas de seguridad y costos necesarios para cada caso en particular.

Cuadro N° 3.1

Determinación de riesgo del servidor

N°	TIPO DE RIESGO	FACTOR DE RIESGO
1		
2		
3		
4		
n		

Fuente: (Borghello, 2007: 200)

Donde:
MA = Muy Alto
A = Alto
M = Medio
B = Bajo
MB = Muy Bajo
Son parámetros del Factor de Riesgo.

La evaluación de riesgos y presentación de respuestas debe prepararse de forma personalizada para cada organización, haciendo un resumen de riesgos y desarrollando las siguientes tareas:

- Niveles de riesgo de los recursos. Los riesgos se clasifican por el nivel de importancia y por la severidad de la pérdida. No se debe llegar a una situación donde se gasta más para proteger aquello que es menos valioso.

Cuadro N° 3.2

Determinación de la severidad de pérdida de los riesgos

RECURSO	RIESGO R_n	IMPORTANCIA I_n	RIESGO EVALUADO RR_n

Muestra el recurso que mas debe protegerse.

Fuente: (Borghello, 2007: 201)

Es necesario determinar los niveles de riesgo mediante factores:

- Estimación del riesgo de pérdida del recurso Ri
- Estimación de la importancia del recurso Ii
- Calcular el riesgo de un recurso RRi = Ri *Ii
- Calcular el Riesgo General (RG) de los recursos del servidor:

$$RG = \frac{(RR_1 + RR_2 + RR_3 + \ldots + RR_n)}{(I_1 + I_2 + I_3 + \ldots + I_n)}$$

- Identificación de amenazas. Corresponde identificar las amenazas y vulnerabilidades que pueden causar bajas en los recursos. Se tienen cuatro tipos de amenazas:

  - Amenazas del entorno (seguridad física). Aplicar controles y mecanismos de seguridad dentro y alrededor de la sala de servidores; para evitar, evaluar y controlar permanentemente:
    - Desastres naturales (terremotos, tormentas eléctricas, inundaciones, humedad)
    - Acceso físico no autorizado.
    - Acciones hostiles (robo, fraude y sabotaje a los activos de la organización)
    - Amenazas ocasionadas por el hombre (electricidad, incendio, humo, ruido eléctrico).

  - Amenazas del sistema (seguridad lógica). Aplicar técnicas y procedimientos que resguarden el acceso a los datos del equipo servidor:
    - Restringir el acceso a los programas y archivos.
    - Asegurar que los usuarios puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
    - Asegurar que se estén utilizado los datos, archivos y programas correctos.
    - Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
    - Que la información recibida sea la misma que ha sido transmitida.
    - Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
    - Disponer de pasos alternativos de emergencia para la transmisión de información.

- Amenazas en la red (comunicaciones). Aplicar controles de acceso a la red y mecanismos para prevenir fallas en comunicaciones y detectar:
  - Agujeros de seguridad en los sistemas operativos.
  - Agujeros de seguridad en las aplicaciones.
  - Errores en las configuraciones de los sistemas.
  - Usuarios que carecen de información respecto al tema.

- Amenazas de personas (insiders-outsiders). Aplicar políticas de acceso físico, lógico y de administración del servidor y la red:
  - Insiders. Personas con acceso a información privilegiada de la organización, como operadores y programadores utilizan sus permisos para alterar archivos o registros.
  - Outsiders. Personas ajenas, ingresan a la red utilizando herramientas cada vez más sofisticadas para explotar agujeros en el diseño, configuración y operación de los sistemas.

Cuadro N° 3.3

Formulario de registro de amenazas

Objetivo. Listar las amenazas y su efecto en los recursos de los servidores de la organización para conocer las vulnerabilidades.			
RECURSO AFECTADO	**AMENAZA**	**VULNERABILIDADES**	**EFECTO**
RECURSO 1	AMENAZA 1	VULNERABILIDAD 1	EFECTO 1
			EFECTO n
		VULNERABILIDAD n	EFECTO 1
			EFECTO n
	AMENAZA n	VULNERABILIDAD 1	EFECTO 1
			EFECTO n
		VULNERABILIDAD n	EFECTO 1
			EFECTO n
RECURSO 2	AMENAZA 1	VULNERABILIDAD 1	EFECTO 1
			EFECTO n
		VULNERABILIDAD n	EFECTO 1
			EFECTO n
	AMENAZA n	VULNERABILIDAD 1	EFECTO 1
			EFECTO n
		VULNERABILIDAD n	EFECTO 1
			EFECTO n

Fuente: Elaboración propia.

3.2.1.2. Gestión de vulnerabilidades.

La gestión de vulnerabilidades es un proceso continuo y automático que mejora la posición de seguridad de la organización. Para este propósito se tiene que evitar al máximo la aparición de vulnerabilidades y más si éstas ya son conocidas. Aplicando correctivos y llevando un registro de hallazgos encontrados, se evita la detección de vulnerabilidades y no se cae en el mismo error, se describe las herramientas utilizadas.

Cuadro N° 3.4

Formulario de registro de gestión de vulnerabilidades

Objetivo. Tener información de puertos, servicios, vulnerabilidades y efectos causados a cada uno de los servidores			
DATOS SERVIDOR:			
NOMBRE DEL SERVIDOR:			
SISTEMA OPERATIVO :			
DIRECCIÓN IP:		NOMBRE DE DOMINIO:	
MASCARA DE SUB RED:		PUERTA DE ENLACE:	
DATOS DE ACTIVIDAD: GESTIÓN DE VULNERABILIDADES			
PUERTO	**PROTOCOLO SERVICIO**	**SERVICIO**	**DETALLE DEL SERVICIO**
ID	**VULNERABILIDAD**	**CORRECTIVO**	**EFECTO (ESTADO)**

Fuente: Elaboración propia en base a Herzog (2007)

Cuadro N° 3.5

Formulario de herramientas utilizadas en la identificación de vulnerabilidades

Objetivo: Listar y describir en que se aplicaran las herramientas a utilizar en el análisis forense.	
SOFTWARE	**DESCRIPCIÓN**

Fuente: Elaboración propia

Las tareas esenciales a realizar son:

- Actualización de S.O. y aplicaciones (parches de seguridad).

- Service packs actualizados para el servidor.
- Configuración segura en el servidor.
- Evitar instalaciones de software por defecto.
- Eliminar demos y aplicativos que no se utilicen (como deshabilitación de servicios y cuentas no utilizados).
- Uso de buenas contraseñas.
- Controlar y realizar una programación responsable de las aplicaciones web que se ejecutan.
- El descubrimiento preciso y exhaustivo de todos los activos y recursos de red utilizando tanto agentes de exploración local como de red.
- El correctivo de vulnerabilidades a través de monitoreo
- La validación de conformidad con las políticas de seguridad de los servidores.
- Utilización de firewalls.
- Análisis periódico de logs.
- Verificación periódica de servicios activos y vulnerabilidades presentes.

3.2.2. Identificación de vulnerabilidades.

Consiste en identificar las vulnerabilidades que cada servidor posee, mediante una planificación, identificación, análisis y gestión.

3.2.2.1. Planificación de vulnerabilidades.

El objetivo principal del proceso de identificación de vulnerabilidades es planificar como se va ha desarrollar el proceso. Para ello:

- Identificar la infraestructura de red (software y hardware) del servidor para monitorear.
- Obtener un historial del servidor:
  - Software instalado
  - Servicios que presta
- Usuario(s) que acceden al servidor y tareas o procesos que realizan.
- Identificar puertos que el servidor esta utilizado para cada aplicación o herramienta.

- Definir fecha y hora para la ejecución de las herramientas de identificación previniendo que no se produzcan bloqueo o interrupciones en los servicios.

Cuadro N° 3.6

Formulario de estructura de red

Objetivo. Conocer los recursos de hardware y software que tiene la organización, lo que permitirá saber información básica de los servidores, el nivel físico de protección y una falla a que servicios o equipos afectara.					
ESTRUCTURA DE RED GRÁFICA DE LA ORGANIZACIÓN:					
DATOS DE ACTIVIDAD: PLANIFICACIÓN DE VULNERABILIDADES.- SERVIDORES DE LA RED.					
SERVIDOR	**SISTEMA OPERATIVO**	**DIRECCION IP**	**NOMBRE DE DOMINIO**	**MASCARA DE SUB RED**	**PUERTA DE ENLACE**

Fuente: Elaboración propia en base a Herzog (2007)

Cuadro N° 3.7

Formulario de registro de servidores

Objetivo. Tener una base de conocimiento de los servidores: puertos que utiliza, usuarios y aplicaciones instaladas. Para contar con una bitácora de los servidores de la organización.			
DATOS SERVIDOR:			
NOMBRE DEL SERVIDOR:			
SISTEMA OPERATIVO :			
DIRECCIÓN IP:		NOMBRE DE DOMINIO:	
MASCARA DE SUB RED:		PUERTA DE ENLACE:	
DATOS DE ACTIVIDAD: PLANIFICACIÓN DE VULNERABILIDADES			
FECHA Y HORA PROGRAMA PARA ESCANEO:			
DEL:		AL:	
SOFTWARE		**DETALLE DEL SOFTWARE**	
SERVICIO		**DETALLE DEL SERVICIO**	
TIPO DE USUARIO	**NOMBRE USUARIO**	**USUARIO**	**TAREAS/ PROCESOS**
PUERTO	**PROTOCOLO**	**APLICACIÓN/HERRAMIENTA**	

Fuente: Elaboración propia en base a Herzog (2007)

3.2.2.2. Identificación de vulnerabilidades planificadas.

Para la identificación de vulnerabilidades en los servidores, es importante realizar escaneos dentro como fuera de la red, porque no se conoce si existen agujeros de seguridad.

- Identificación de vulnerabilidades internas. Un entorno privilegiado, al estar dentro de la red consumiendo los recursos y servicios prestados por los servidores. Se tiene los permisos necesarios para poder ejecutar herramientas que realizan escaneo de vulnerabilidades.

  Las herramientas de identificación de vulnerabilidades internas son las que se utilizan para determinar agujeros de seguridad existentes y niveles de parcheado de los sistemas. Además, cada una utiliza su particular método de detección por lo que se recomienda utilizar más de una herramienta, como:

  - ISS System Scanner
  - Nessus
  - Nmap

  Los resultados deben registrarse en una tabla para realizar un análisis minucioso del servidor y su estado actual de manera que se pueda identificar si se trata de una vulnerabilidad o una falsa alarma.

Cuadro N° 3.8
Formulario de registro de vulnerabilidades internas

Objetivo. Tener un registro de los resultados obtenidos de la aplicación de las diferentes herramientas utilizadas para el escaneo interno de los servidores.		
DATOS SERVIDOR:		
NOMBRE DEL SERVIDOR:		
SISTEMA OPERATIVO:		
DIRECCIÓN IP:	NOMBRE DE DOMINIO:	
MASCARA DE SUB RED:	PUERTA DE ENLACE:	
DATOS DE ACTIVIDAD: IDENTIFICACIÓN DE VULNERABILIDADES INTERNAS		
ID	**HERRAMIENTA**	**VULNERABILIDAD**

Fuente: Elaboración propia en base a Herzog (2007)

- Identificación de vulnerabilidades externas. Un entorno no privilegiado porque se busca acceder a recursos de los servidores vía internet para detectar todas las posibles vulnerabilidades que podrían ser utilizadas por los intrusos (hackers, virus, crackers, etc.) con el fin de explotar o causar daño a recursos y servicios de los servidores.

  Esta tarea se lo realiza desde una conexión fuera de la red utilizando herramientas de detección de vulnerabilidades externas para buscar agujeros por donde se podrían presentar incidentes. Las herramientas que podrían utilizarse son:

  - ISS Internet Scanner
  - Nessus Security Scanner
  - Retina Netwok Security Scanner

  Es recomendable utilizar más de una herramienta, cada una da como resultado un listado detallado de vulnerabilidades que deben registrarse en una tabla para su posterior análisis, corrección y reporte de hallazgos.

Cuadro N° 3.9

Formulario de registro de vulnerabilidades externas

Objetivo. Tener un registro de los resultados obtenidos de la aplicación de las diferentes herramientas utilizadas para el escaneo externo de los servidores.		
DATOS SERVIDOR:		
NOMBRE DEL SERVIDOR:		
SISTEMA OPERATIVO:		
DIRECCIÓN IP:	NOMBRE DE DOMINIO:	
MASCARA DE SUB RED:	PUERTA DE ENLACE:	
DATOS DE ACTIVIDAD: IDENTIFICACIÓN DE VULNERABILIDADES EXTERNAS		
ID	**HERRAMIENTA**	**VULNERABILIDAD**

Fuente: Elaboración propia en base a Herzog (2007)

3.2.2.3. Análisis de vulnerabilidades.

Los resultados obtenidos de la aplicación de herramientas de detección de vulnerabilidades internas y externas deben ser analizados y evaluados, porque no puede dependerse ni aceptarse

un solo resultado. Una vez analizado, se procede a listar las vulnerabilidades aceptadas en la Tabla de registro de Vulnerabilidades.

Cuadro N° 3.10

Formulario de registro de análisis de vulnerabilidades

Objetivo. Conocer el análisis realizado a cada una de las vulnerabilidades listadas por las herramientas, para desechar aquellas falsas vulnerabilidades.			
DATOS SERVIDOR:			
NOMBRE DEL SERVIDOR:			
SISTEMA OPERATIVO:			
DIRECCIÓN IP:		NOMBRE DE DOMINIO:	
MASCARA DE SUB RED:		PUERTA DE ENLACE:	
DATOS DE ACTIVIDAD: IDENTIFICACIÓN DE VULNERABILIDADES INTERNAS			
ID	**HERRAMIENTA**	**VULNERABILIDAD**	**OBSERVACION (ANÁLISIS)**

Fuente: Elaboración propia en base a Herzog (2007)

3.2.2.4. Búsqueda y verificación de vulnerabilidades reales.

Analizado las vulnerabilidades internas y externas corresponde separar los falsos positivos y los falsos negativos de las vulnerabilidades reales, en base a todo el conjunto presentado por las diferentes herramientas utilizadas, es decir; con cada reporte analizado corresponde identificar, comprender y verificar vulnerabilidades, errores de configuración. Por lo que se sugiere:

- Integrar en las pruebas realizadas los escáneres, herramientas de hacking y exploits utilizados actualmente.
- Determinar y clasificar las vulnerabilidades por tipo de aplicación y sistema operativo.
- Ajustar las vulnerabilidades a servicios.
- Determinar el tipo de aplicación y servicio por vulnerabilidad.
- Realizar la identificación de vulnerabilidades internas como externas con al menos 2 escáneres automáticos de vulnerabilidades.
- Identificar todas las vulnerabilidades relativas a las aplicaciones.

- Identificar todas las vulnerabilidades relativas a los sistemas operativos.
- Identificar todas las vulnerabilidades de sistemas parecidos o semejantes que podrían también afectar a los demás servidores.
- Verificar todas las vulnerabilidades encontradas durante la fase de búsqueda de exploits con el objetivo de descartar falsos positivos y falsos negativos.
- Verificar todos los positivos (vulnerabilidades encontradas).

La información detectada como vulnerabilidad o los sitios que llevan el reporte de vulnerabilidades, mas datos del servidor, deberán registrarse en un formulario para documentar.

Cuadro N° 3.11

Formulario de registro de búsqueda y verificación de vulnerabilidades reales

Objetivo. Tener un registro de la búsqueda y verificación de cada vulnerabilidad real para cada servidor.		
DATOS SERVIDOR:		
NOMBRE DEL SERVIDOR:		
SISTEMA OPERATIVO:		
DIRECCIÓN IP:	NOMBRE DE DOMINIO:	
MASCARA DE SUB RED:	PUERTA DE ENLACE:	
DATOS DE ACTIVIDAD: BÚSQUEDA Y VERIFICACIÓN DE VULNERABILIDAD REALES.		
FECHA:		
DETALLE DEL SERVICIO	**SERVICIO**	**PUERTO**
ID	**VULNERABILIDAD**	**ESTADO**

Fuente: Elaboración propia en base a Herzog (2007)

3.2.3. Corrección de vulnerabilidades.

Verificado las vulnerabilidades reales de los equipos servidores corresponde corregir de manera correcta, ágil y oportuna. Deberá registrarse la corrección de vulnerabilidades de cada servidor para tener un registro del estado actual de la seguridad.

3.2.3.1. Búsqueda de correctivos.

Identificada las vulnerabilidades de los servidores, para cada vulnerabilidad encontrada se procede con la búsqueda de correctivos, basado en el reporte de verificación y búsqueda. A manera de referencia se menciona que existen sitios que llevan reporte de vulnerabilidades:

- http://www.seguridad.unam.mx/vulnerabilidadesDB
- http://www.vnunet.es/Seguridad/Vulnerabilidades
- http://www.alerta-antivirus.es/seguridad/busca_vulns.php

Cuadro N° 3.12

Formulario de registro de la corrección de vulnerabilidades

Objetivo. Tener una bitácora de los escaneos de vulnerabilidades y de la correcta atención a cada vulnerabilidad encontrada.			
DATOS SERVIDOR:			
NOMBRE DEL SERVIDOR:			
SISTEMA OPERATIVO :			
DIRECCIÓN IP:		NOMBRE DE DOMINIO:	
MASCARA DE SUB RED:		PUERTA DE ENLACE:	
DATOS DE ACTIVIDAD: BÚSQUEDA Y VERIFICACIÓN DE VULNERABILIDAD REALES.			
FECHA:			
PUERTO	**PROTOCOLO SERVICIO**	**SERVICIO**	**DETALLE DEL SERVICIO**
ID	**VULNERABILIDAD**	**CORRECTIVO**	**EFECTO (ESTADO)**

Fuente: Elaboración propia en base a Herzog (2007)

3.2.3.2. Informe final y presentación de la información.

La documentación elaborada en cada una de las etapas (registros de vulnerabilidades y correctivos) debe prepararse para un informe final con las respectivas conclusiones y recomendaciones, adjuntando un resumen de vulnerabilidades de cada servidor en términos no técnicas. Terminado el informe debe ser presentado.

Cuadro N° 3.13

Formulario de informe final de vulnerabilidades encontradas en el servidor

Objetivo. El presente informe describe información no técnica de las vulnerabilidades encontradas en las computadoras servidores de la organización, para dar información resumida y clara del proceso final de identificación de vulnerabilidades.

1. INFORMACIÓN GENERAL.

Nombre de la Organización: _____

Responsable equipo servidor:
Área: _____ Unidad: _____
Nombres y Apellidos: _____
E-mail:_____ Teléfono/Celular: _____

2. INFORMACIÓN SOBRE EL EQUIPO.

Nombre del equipo: _____ Dirección IP: _____
Sistema operativo (nombre y versión): _____
Administración y servicios que realiza: _____
_____
Información procesada: _____

Estado Anterior del servidor (Antes de la corrección de vulnerabilidades):

_____

Correcciones realizadas para salvar las vulnerabilidades del servidor:
_____
_____

Estado Actual del servidor (Después de la corrección de vulnerabilidades):
_____
_____

Observaciones:
_____
_____

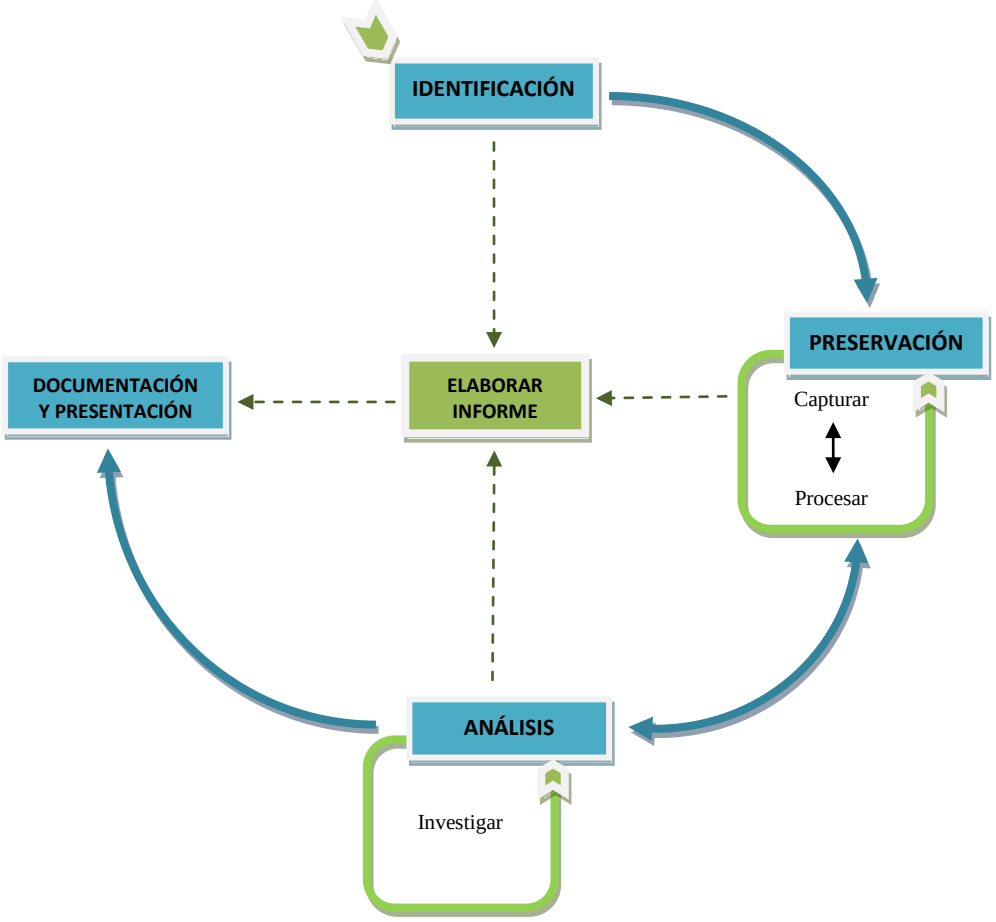
Fuente: Elaboración propia

3.3. Metodología para el análisis forense.

La presente metodología permite realizar análisis forense a equipos servidores de una organización, su aplicación no restringe introducir otros procesos, subprocesos o algunas tareas, queda abierta a una interpretación en la que una nueva tecnología sea introducida.

La metodología tiene un proceso iterativo y repetitivo con cuatro fases, cada una se realimenta de la fase anterior. El proceso inicia con la fase de identificación, progresa hacia la fase de preservación que es un proceso repetitivo e iterativo permitiendo capturar y procesar la evidencia, esta fase interactúa con la fase de análisis que igualmente es un proceso repetitivo e iterativo permitiendo realizar la investigación. En cada una de estas fases se elabora un informe que en la última fase se documenta y presenta para establecer la reconstrucción.

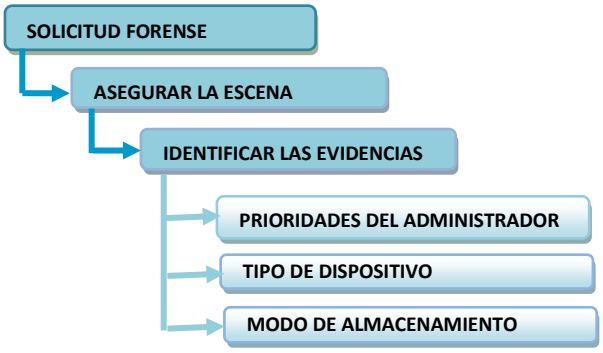
Gráfico Nº 3.6
Proceso de análisis forense



Fuente: Elaboración Propia

Cada fase contiene actividades, algunas dependen de la anterior actividad, tal como se muestra en los siguientes cuatro gráficos.

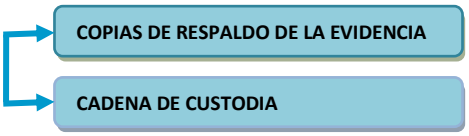
Gráfico Nº 3.7
Fase I: Identificación de la evidencia



Fuente: Elaboración Propia

Gráfico Nº 3.8

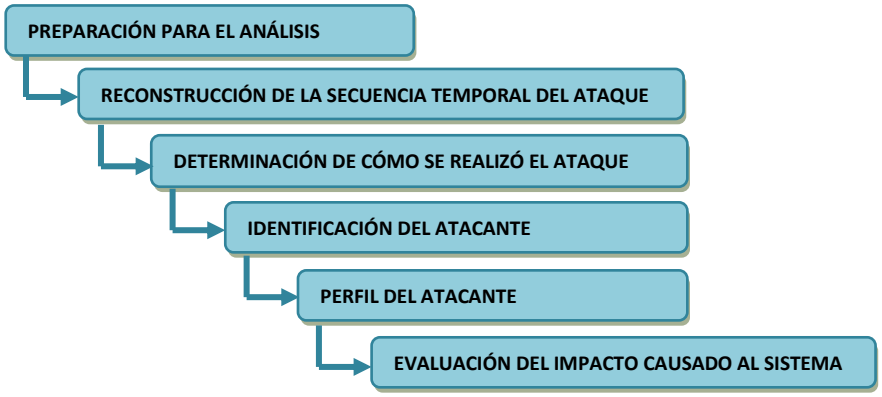
Fase II: Preservación de la evidencia



Fuente: Elaboración Propia

Gráfico Nº 3.9

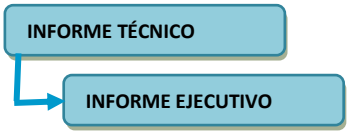
Fase III: Análisis de la evidencia



Fuente: Elaboración Propia

Gráfico Nº 3.10

Fase IV: Documentación y presentación



Fuente: Elaboración Propia

3.3.1. Identificación de la evidencia.

En esta fase el investigador forense debe identificar a todos los objetos que tengan valor como evidencia para posteriormente recolectarlos, reconociendo la frágil naturaleza de los datos digitales, la actividad termina con un plan a seguir. Aquí se pregunta:

- ¿Qué tipo de información está disponible?
- ¿Cómo la podemos "llevar" de forma segura?
- ¿Qué puede formar parte de la evidencia?

3.3.1.1. Solicitud forense.

El administrador del equipo servidor con la aprobación de la parte directiva de la organización, debe presentar un documento notificando la ejecución de un incidente, solicitando la revisión del mismo y toda la información necesaria para dar inicio al proceso de análisis forense.

Cuadro N° 3.14

Formulario de solicitud forense

Objetivo. La presente solicitud describe toda la información del incidente ocurrido con el servidor de la organización.

1. DESCRIPCIÓN DEL DELITO INFORMÁTICO.

Fecha del incidente:_____
Duración del incidente (si se puede establecer):_____
Detalles del incidente:_____
_____
Como se descubrió el incidente:_____
Otros aspectos que se consideren importantes en el incidente, describir:_____
_____

2. INFORMACIÓN GENERAL.

Área:_____ Nombre de la dependencia:_____

Responsable equipo servidor (sistema afectado):
Nombres y Apellidos: _____
Cargo: _____ E-mail:_____
Teléfono:_____ Celular: _____ Fax:_____

Si sabe de otro equipo o sistema que haya sufrido el mismo problema o uno similar:_____
_____

3. INFORMACIÓN DEL SERVIDOR (EQUIPO AFECTADO).

Nombre del servidor:_____ Dirección IP:_____
Marca:_____ Modelo:_____
Capacidad de la RAM:_____
Capacidad del disco duro:_____
Modelo del Procesador:_____
Sistema operativo (nombre y versión):_____
Función del equipo:_____
_____
Tipo de información procesada por el servidor:_____

Usuarios:_____
_____
Servicios:_____
_____
Observaciones:_____
_____

4. ESTRUCTURA DE RED GRÁFICA DE LA ORGANIZACIÓN CON RESPECTO AL SERVIDOR:

Fuente: Elaboración Propia

3.3.1.2. Asegurar la escena.

Implica actuar de forma metódica y profesional sin borrar huellas para asegurar un buen proceso de análisis forense del servidor; es decir, este proceso debe realizar personal competente con el fin de garantizar y asegurarse que los procesos como las herramientas a utilizar sean las más idóneas. Además, de rotular las evidencias.

Cuadro N° 3.15

Formulario de rotulo de evidencias

Objetivo: Registrar información de la evidencia encontrada.	
N°	
CASO	
FECHA	
HORA	
TIPO	
OBSERVACIONES	
FIRMA	

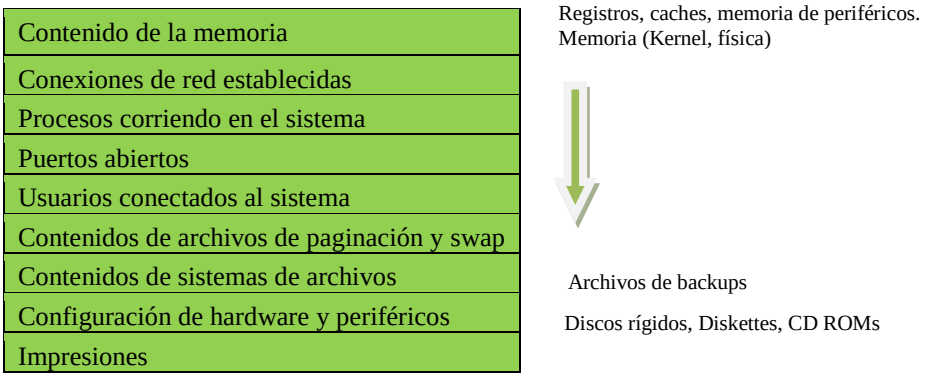
Fuente: Elaboración propia

3.3.1.3. Identificar las evidencias.

La identificación de la evidencia presentada (el servidor), que es la escena del crimen, está sujeta a todos los procesos necesarios para la presentación de resultados finales.

Esta tarea comprende la identificación, búsqueda y recopilación de evidencias. Se debe identificar qué cosas pueden ser evidencias, dónde y cómo está almacenada, qué sistema operativo se está utilizando. A partir de este paso se puede identificar los procesos para la recuperación de evidencias adecuadas, así como las herramientas a utilizar.

Como regla general se debe obtener la evidencia de la forma menos destructiva posible, y siempre en orden de más volátil a menos volátil, específicamente en el orden que se muestra a continuación.



La evidencia se clasifica en:

- Prioridades del administrador**.** De acuerdo a las prioridades del administrador de servidor, puede calcularse la criticidad de los daños producidos por el incidente, una forma de clasificar es aplicando la formula:

CRITICIDAD DE LOS DAÑOS	=	Extensión de daños producidos	+	Criticidad de los recursos afectados

Donde:

- La extensión de los daños producidos es:
  - Grave: cuando el incidente produjo daños muy severos sobre los servicios o información.
  - Moderado: cuando el incidente causo molestias y pérdida de información.
  - Leve: cuando el incidente producido no tiene mayor importancia, no se produjo ningún tipo de perdida pero si un corte o molestia en los servicios.

- La criticidad de los recursos afectados es:
  - Alta: cuando los recursos afectados son muy importantes dentro de la organización y como tal comprometen el normal funcionamiento y prestación de servicios.
  - Media: cuando los recursos afectados causan molestias a un área de la organización.
  - Baja: los recursos afectados causan ciertas molestias pero se puede seguir con el normal funcionamiento de los equipos.

Los datos obtenidos deberán ser registrados en formularios.

Cuadro N° 3.16

Formulario de daños producidos y recursos afectados

Objetivo: Tener información de los efectos del incidente y recursos afectados del servidor.						
INCIDENTE	**EXTENSIÓN DE DAÑOS PRODUCIDOS**			**CRITICIDAD DE LOS RECURSOS AFECTADOS**		
	GRAVE	**MODERADO**	**LEVE**	**ALTA**	**MEDIA**	**BAJA**

Fuente: Elaboración Propia

Cuadro N° 3.17

Formulario de criticidad de los daños

Objetivo: Tener información de la criticidad de los daños del servidor por efecto de un incidente que causo daños y afecto recursos. Además de obtener la prioridad de los incidentes según el administrador.		
INCIDENTE	**CRITICIDAD DE LOS DAÑOS**	**PRIORIDAD**

Fuente: Elaboración Propia

Donde:

Parámetros del factor de criticidad de los daños son:

Grave + Alta = Muy Grave
Grave + Media = Grave
Grave + Baja = Moderado
Moderado + Alta = Grave
Moderado + Media = Moderado
Moderado + Baja = Leve
Leve + Alta = Moderado
Leve + Media = Leve
Leve + Baja = Leve

Prioridad es el nivel de importancia de un incidente que se evalúa en una escala del 1 al 10, entonces:

Muy Grave = 10
Grave = 7
Moderado = 4
Leve = 1

- Tipo de dispositivo**.** La identificación también va referido al tipo de dispositivo:

  - Sistemas informáticos
  - Redes
  - Otros dispositivos

- Modo de almacenamiento**.** También se toma en cuenta el modo de almacenamiento en la identificación de evidencias, porque va referido a:

  - Almacenamiento volátil. Información que se pierde al apagar el equipo como: hora del sistema, contenido de la memoria, procesos en ejecución, programas en ejecución, usuarios conectados, configuración de red, conexiones activas, puertos abiertos, etc.
  - Almacenamiento no volátil. Medios físicos de almacenamiento como memorias usb, CD, discos duros.

3.3.2. Preservación de la evidencia.

Es parte de la investigación forense que se enfoca en resguardar los objetos que tengan valor como evidencia de manera que estos permanezcan de forma completa, clara y verificable. Aquí se utiliza técnicas criptográficas como códigos de integridad (función hash, checksums) para autenticar todos los archivos e imágenes utilizadas. Se debe llevar la más prolija documentación de cómo ha sido preservada la evidencia tras la recopilación.

En esta fase, es imprescindible definir los métodos adecuados para el almacenamiento y etiquetado de las evidencias, también la utilización de herramientas.

Cuadro N° 3.18

Formulario de herramientas utilizadas en el análisis forense

Objetivo: Listar y describir en que se aplicaran las herramientas a utilizar en el análisis forense.	
SOFTWARE	**DESCRIPCIÓN**

Fuente: Elaboración propia

3.3.2.1. Copias de la evidencia.

Las copias de la evidencia van relacionado al estado en que se encuentra el servidor, si este fue apagado o después del incidente ocurrido aun se encuentra prendido.

Un primer paso es realizar un by-pass del sistema operativo y crear por "fuera" un backup de toda la evidencia. Posteriormente, realizar dos copias de las evidencias obtenidas y generar una suma de comprobación de la integridad de cada copia mediante el empleo de funciones hash tales como MD5 o SHA1. Incluir estas firmas en la etiqueta de cada copia de la evidencia sobre el propio medio de almacenamiento como CD o DVD etiquetando la fecha y hora de creación de la copia, nombrar cada copia ("copia A", "copia B") para distinguirlas claramente del original.

Si además se extrae los discos duros del sistema para utilizarlos como evidencia, se debe seguir el mismo procedimiento, colocando sobre ellos la etiqueta evidencia original, incluir además las correspondientes sumas hash, fecha y hora de la extracción del equipo, datos de la persona que realizó la operación, fecha, hora y lugar donde se almacenó.

Tener en cuenta que existen factores externos como cambios bruscos de temperatura o campos electromagnéticos que pueden alterar la evidencia. Toda precaución es poca, incluso si se decide enviar los discos a que sean analizados por empresas especializadas.

Cuadro N° 3.19

Formulario de control de copias de evidencias

Objetivo: Mencionar actividades de copias de evidencia que se realizaron.			
ACTIVIDAD	**SI**	**NO**	**OBSERVACIÓN**

Fuente: Elaboración propia

3.3.2.2. Cadena de custodia.

La cadena de custodia implica que el acceso a la evidencia sea muy restrictivo quedando claramente documentado, posibilitando detectar y pedir responsabilidades ante manipulaciones incorrectas, intentos de acceso no autorizados o que algún otro dispositivo electromagnético se use dentro de un determinado radio.

En esta etapa se establecen las responsabilidades y controles de cada una de las personas que manipulan la evidencia. Se debe preparar un documento en el que se registren los datos personales de todos los implicados en el proceso de manipulación de las copias, desde que se tomaron hasta su almacenamiento. El documento debe contener la siguiente información:

- Dónde, cuándo y quién examinó la evidencia, incluyendo su nombre, su cargo, un número identificativo, fechas y horas, etc.
- Quién estuvo custodiando la evidencia, durante cuanto tiempo y dónde se almacenó.
- Cuando se cambie la custodia de la evidencia también se deberá documentar cuándo y como se produjo la transferencia y quién la transportó.

Cuadro N° 3.20

Formulario de cadena de custodia

Objetivo: Describir la ubicación de la evidencia y su traslado.					
N°	**UBICACIÓN ACTUAL**	**FECHA**	**RAZON DE TRASLADO**	**SITIO A DONDE SE TRASLADA**	**OBSERVACIONES (quién, sus datos)**
LUGAR DE DEPÓSITO FINAL DE LA EVIDENCIA:				**FECHA:**	

Fuente: Elaboración propia

3.3.3. Análisis de la evidencia.

En esta fase es donde el investigador busca filtrar todos los objetos recolectados y preservados de la escena del delito a fin de separar los objetos que no tienen valor como evidencia de los que sí. Se emplean las herramientas propias del sistema operativo (anfitrión) y las que se prepararon en la fase de extracción y preparación.

Obtenida las evidencias digitales recopiladas y almacenadas de forma adecuada, inicia el análisis forense, cuyo objetivo es reconstruir con todos los datos disponibles la línea temporal del ataque, determinando la cadena de acontecimientos que tuvieron, lugar del inicio de ataque hasta el momento de su descubrimiento. Esto termina cuando se descubra cómo se produjo el ataque, quién o quienes lo llevaron a cabo, bajo qué circunstancias se produjo, cuál era el objetivo del ataque, qué daños causaron, etc.

3.3.3.1. Preparación para el análisis.

El investigador forense, debe:

- Acondicionar un entorno de trabajo adecuado al estudio que se desea realizar
- Trabajar con las imágenes que se recopiló como evidencias, o mejor aún con una copia de éstas, tener en cuenta que es necesario montar las imágenes tal cual estaban en el sistema comprometido.
- Preparar dos estaciones de trabajo, una de ellas contendrá al menos dos discos duros.
- Instalar un sistema operativo que actuará de anfitrión y servirá para realizar el estudio de las evidencias. En este mismo ordenador y sobre un segundo disco duro, instalar las imágenes manteniendo la estructura de particiones y del sistema de archivos tal y como estaban en el equipo atacado.
- En otro equipo instalar un sistema operativo configurado exactamente igual que el equipo atacado, además mantener nuevamente la misma estructura de particiones y ficheros en sus discos duros.

3.3.3.2. Reconstrucción de la secuencia temporal del ataque.

Montadas las imágenes del sistema atacado en un ordenador independiente con un sistema operativo anfitrión de confianza, se procede a reconstruir la secuencia temporal del ataque ejecutando las siguientes tareas:

- Crear una línea temporal o time line de sucesos, recopilando información de los ficheros:

  - Marcas de tiempo MACD (fecha y hora de modificación, acceso, creación y borrado).
  - Ruta completa.
  - Tamaño en bytes y tipo de fichero.
  - Usuarios y grupos a quien pertenece.
  - Permisos de acceso.
  - Si fue borrado o no.

- Buscar ficheros y directorios que han sido creados, modificados o borrados recientemente, o instalaciones de programas posteriores a la del sistema operativo y que además se encuentren en rutas poco comunes. Pensar que la mayoría de los atacantes y sus herramientas crearán directorios y descargarán sus "aplicaciones" en lugares donde no se suele mirar, como por ejemplo en los directorios temporales:

  - Examinar con detalle los ficheros logs y registros que se examinaron durante la búsqueda de indicios del ataque, intentar buscar una correlación temporal entre eventos.
  - Examinar los fragmentos del archivo /var/log/messages, que es donde se detectan y registran los accesos FTP.

Realizada estas tareas es conveniente describir la identificación de la imagen, las características del sistema operativo, procesos, servicios y aplicaciones.

3.3.3.3. Determinación de cómo se realizó el ataque.

Consiste en averiguar qué vulnerabilidad o fallo de administración causó el agujero de seguridad y que herramientas utilizó el atacante para aprovecharse. La información se consigue empleando herramientas y una combinación de consultas a los archivos logs, registros, claves, cuentas de usuarios, etc.

Las siguientes actividades permiten conocer que acciones realizo el atacante:

- Cuando el sistema esta aun funcionando, revisar los servicios y procesos abiertos que se recopilaron como evidencia volátil, así como los puertos TCP/UDP y conexiones que estaban abiertas.
- Si se tiene claro la vulnerabilidad que dejó el sistema desprotegido, buscar en Internet algún exploit anterior a la fecha del incidente que utilice esa vulnerabilidad.
- Comprobar si la ejecución del exploit sobre una máquina igual que la afectada, genera los mismos eventos de evidencias.

3.3.3.4. Identificación del atacante.

Para este propósito se consulta nuevamente algunas evidencias volátiles que se recopiló en las primeras fases. Revisar conexiones que estaban abiertas, en qué puertos y qué direcciones IP las solicitaron, buscar entre las entradas a los logs de conexiones. También se puede indagar entre los archivos borrados que se recuperó por si el atacante eliminó alguna huella.

Para esta tarea se puede usar herramientas como nmap, para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando, etc.

3.3.3.5. Perfil del atacante.

Determinar el perfil del atacante, pudiendo ser:

- Hackers
- SciptKiddies
- Profesionales
- Personal interno
- Expersonal interno

3.3.3.6. Evaluación del impacto causado al sistema.

El análisis forense permite investigar qué es lo que han hecho los atacantes una vez que accedieron al sistema, si son efectos negativos de tipo técnico, si los ataques al sistema atacado son críticos; con esto se realiza una estimación del impacto causado. Por ejemplo, ataques al corta fuegos, router de conexión a internet o intranet, servidor web y servidores de bases de datos, tendrán diferente repercusión según el tipo de servicio que prestan los servidores.

Generalmente se pueden dar dos tipos de ataques:

- Ataques pasivos. Son los que no alteran la información ni la operación normal de los sistemas, limitándose a fisgonear.
- Ataques activos. Son los que alteran seriamente tanto la información como la capacidad de operación del sistema.

3.3.4. Documentación y presentación de pruebas.

Es la fase final de la investigación forense, se presentan los resultados y hallazgos del investigador. La presentación debe ser entendible y convincente, es decir; aquí se debe reseñar los procedimientos y las técnicas utilizadas para recolectar, preservar y filtrar la evidencia de manera que exista certidumbre en los métodos usados, aumentado así la credibilidad del investigador en un contra examen de los mismos.

Se presentan dos informes: el técnico y el ejecutivo. La documentación elaborada (los formularios) en cada una de las fases debe ser fechada y agregado al informe técnico.

3.3.4.1. Informe técnico.

El informe técnico contiene un detalle del análisis efectuado, describe en profundidad la metodología, técnicas y hallazgos del equipo forense. También incluye los formularios registrados en cada una de las fases. Por lo general su redacción es más de 60 hojas con el siguiente contenido:

Cuadro N° 3.21

Formulario del contenido de un informe técnico

Objetivo: Dar información que proporciona una idea de los puntos que debe detallar un informe técnico.
▪ Introducción ▪ Antecedentes del incidente ▪ Recolección de los datos ▪ Descripción de la evidencia ▪ Entorno del análisis - Descripción de las herramientas ▪ Análisis de la evidencia - Información del sistema analizado ◆ Características del SO ◆ Aplicaciones ◆ Servicios ◆ Vulnerabilidades ◆ Metodología - Descripción de los hallazgos ◆ Huellas de la intrusión ◆ Herramientas usadas por el atacante ◆ Alcance de la intrusión ◆ El origen del ataque ▪ Cronología de la intrusión ▪ Conclusiones ▪ Recomendaciones específicas ▪ Referencias ▪ Anexos

Fuente: Elaboración Propia

3.3.4.2 Informe ejecutivo.

El informe ejecutivo contiene en lenguaje común (explicación no técnica) un resumen de los hechos más destacables de lo ocurrido en el sistema analizado. Este informe es de especial interés para exponer lo sucedido al personal no especializado en sistemas informáticos, como al responsable de recursos humanos, administración e incluso directivos. Consta de pocas páginas, entre tres y cinco, con el siguiente contenido:

Cuadro N° 3.22

Formulario del contenido de un informe ejecutivo

Objetivo: Dar información que proporciona una idea de los puntos que debe detallar un informe ejecutivo.
▪ Introducción ▪ Análisis ▪ Sumario del incidente ▪ Principales Conclusiones del análisis ▪ Solución al incidente ▪ Recomendaciones finales

Fuente: Elaboración Propia

CAPÍTULO IV

RESULTADOS DE LA APLICACIÓN DE LA METODOLOGÍA PROPUESTA

El capítulo expone una explicación práctica de la metodología propuesta, habiendo seleccionado el servidor de una institución educativa para su aplicación. Dando así cumplimiento al tercer objetivo específico planteado y demostrar los resultados de la investigación.

4.1. E.S.F.M. "E.A.".

Para validar y verificar la metodología desarrollada, fue necesario determinar la organización donde se aplicara la metodología, la muestra poblacional a partir de la población de estudio, las técnicas e instrumentos para la recolección de datos en la investigación. Habiendo seleccionado a la E.S.F.M. "E.A.", que por razones de seguridad se omite el nombre completo de la institución y nombres del personal. Esta es una institución educativa que tiene por misión formar maestros profesionales de la educación con sólidas competencias disciplinares, psicopedagógicas, didácticas e interculturales que responden crítica y reflexivamente a los desafíos del entorno a través de una gestión de calidad para desarrollar una educación integral de excelencia en las unidades educativas del sistema educativo nacional. Su visión es ser una institución formadora de maestros profesionales de excelencia con competencias profesionales de calidad que contribuyen al desarrollo político, económico, social y cultural a nivel local, regional y nacional.

En el año 1979 la Federación de Maestros Urbanos de Potosí, viendo la necesidad de facilitar a los estudiantes potosinos el acceso al estudio como maestros en educación, planteó la necesidad de crear una escuela normal en esta ciudad. Contra toda adversidad después de largos trámites y viajes a la ciudad de La Paz, el gobierno departamental emite la resolución Nº 002 creando la institución denominada "E.N.E.A.". El 1º de abril de 1985 bajo Decreto Supremo Nº 20747 abre sus puertas y es reconocida a nivel nacional por el gobierno del Dr. Hernán Siles Suazo.

4.1.1. Diagnostico de la situación actual.

La institución es dependiente del Ministerio de Educación desde hace 6 años, se destaca a nivel nacional como una de las mejores, tiene una población de 1500 alumnos distribuidos en diferentes especialidades, 104 profesores docentes, 3 directores, 27 funcionarios administrativos que incluye al administrador del servidor y 6 funcionarios de servicio.

La institución tiene 120 computadoras; de estas 6 son computadoras portátiles que en casos excepcionales se prestan temporalmente a los docentes por la unidad de bienes y servicios. El resto están distribuidos dentro la institución, 111 como equipos clientes y 3 están configurados como servidores para administrar accesos de usuarios, bases de datos y servicio de internet.

La institución cuenta con el servicio de internet, tanto profesores como alumnos utilizan este servicio para buscar información personal o realizar investigación, en promedio una hora por día acceden al servicio de internet. Mientras los directores y administrativos tienen acceso continúo a internet y otros servicios administrados por los 3 servidores de la institución, motivo por el cual se determino mediante el método no probabilístico la muestra poblacional de 30 personas (ver Anexo Nº 6).

La muestra seleccionada, se sometió a la investigación científica mediante los métodos empíricos con el fin de obtener información real y exacta. Basado en los indicadores determinados en la operacionalización de variables, se elaboró un cuestionario de encuesta con preguntas múltiples (ver Anexo Nº 7) y un cuestionario de entrevista (ver Anexo Nº 8), así mismo se elaboró un formulario de observación (ver Anexo Nº 9).

Respondido el cuestionario de la encuesta, con el propósito de medir los resultados se realizo la recolección del instrumento y se procedió con la tabulación de los resultados de cada uno de los ítems planteados, luego se realizó la representación porcentual en cuadros y gráficas estadísticas para finalmente hacer el análisis e interpretación de los resultados obtenidos (ver Anexo Nº 10) con el fin de determinar si correspondía aplicar la metodológica propuesta en la institución, además de obtener información para la investigación.

4.1.2. Justificativo del trabajo en la E.S.F.M. “E.A.”.

La E.S.F.M. “E.A.” en las últimas fechas se vio afectada por un siniestro informático, se desconocía de donde se originó, sin embargo se conocía lo que ocasionaba:

- Servidores. Bajo rendimiento en la velocidad de arranque del sistema operativo, procesamiento de datos, ejecución de archivos y otros sistemas; afectando en la disponibilidad del servidor y tiempo de respuesta con los demás equipos de la red. Los antivirus instalados en cada servidor detectaban programas maliciosos y accesos no autorizados. Razones por la que el administrador solía liberar memoria reiniciando el servidor afectado.
- Computadoras clientes. Se necesitaba varios minutos para iniciar el sistema operativo, conectarse a la red y acceder a un servicio de los servidores. Se tenían accesos no autorizados, activación y ejecución de programas maliciosos en cada uno de los equipos, de repente quedaban bloqueados. Motivo por el cual los usuarios solían apagar, reiniciar o desinfectar su ordenador.
- Servicio de Internet. Problemas de conexión, problemas de acceso a ciertas direcciones web y baja velocidad en la transmisión de datos.

El personal alarmado por esta situación, solicitó se efectúe un estudio e investigación hasta lograr identificar a los responsables del suceso, además de prevenir este tipo de situaciones con el fin de optimizar las actividades laborales.

El administrador del servidor, como responsable del sistema informático asumió como prioridad principal solucionar este problema, tenía la sospecha de problema de virus, además afirmaba que era imposible acceder a los equipos clientes y servidores al estar configurados para evitar accesos no autorizados, salvo lo permita el usuario.

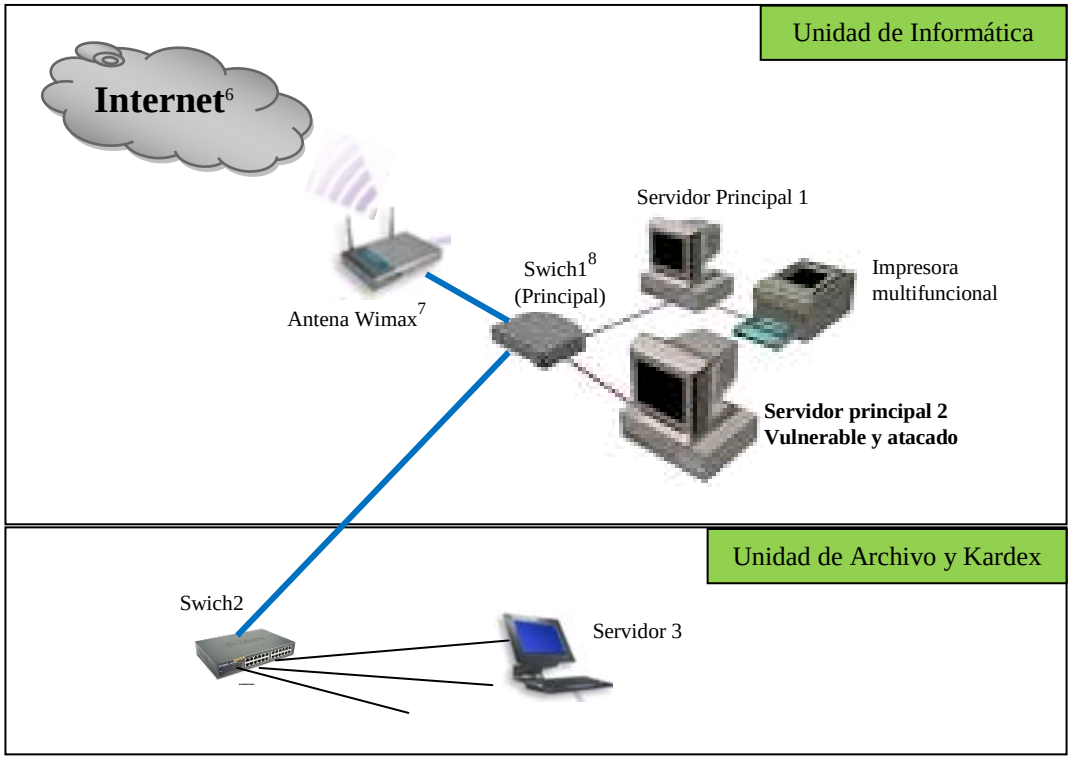
Por la magnitud del problema informático suscitado e información proporcionada por el administrador con respecto a los servidores (información almacenada, servicios que prestan, porcentaje de utilización, frecuencia de problemas, fallas, entre otros), se delimito investigar lo sucedido en el equipo servidor-2.

4.1.3. Entorno de red y análisis de los servidores.

En el Gráfico N° 27 se muestra la red de computadoras de la institución con respecto a sus equipos servidores, estando dos servidores ubicados físicamente en la unidad de informática y otro en la unidad de archivo y kardex.

Gráfico N° 4.1

Arquitectura de red con respecto al servidor atacado



Fuente: Elaboración propia en base a información obtenida de la totalidad de computadoras conectadas físicamente en red (información proporcionada por el administrador del servidor)

Tal como se muestra en la grafica, aunque parece inverosímil no se tiene medidas de seguridad como un corta fuegos u otro dispositivo, además los servidores son equipos normales sin ninguna configuración especial de restricciones y protección. Dicha situación es real en muchas otras organizaciones.

[6]Internet: conjunto descentralizado de redes de comunicación interconectados, utilizan la familia de protocolos TCP/IP, es de alcance mundial.

[7]Wimax: atiende a *World Wide Interoperability for Microwave Access*, que significa interoperabilidad mundial para acceso por microondas. También recibe el nombre de 802.16 dado por la IEEE. Wimax tiene el potencial para dar acceso a internet, banda ancha.

[8]Switch: se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las redes de área local.

La instalación física del cableado cumple con estándares internacionales de diseño de redes, pero no se tienen normas de seguridad internas o externas, ni políticas de seguridad para los distintos usuarios, por lo que estos asumen que nada esta prohibido, salvo cuando existe una recomendación verbal o el sistema da un mensaje de advertencia de no poseer permiso de acceso o ejecución de algún programa.

Con respecto a los servidores, el servidor-1 esta configurado para administrar servicio de internet, la pagina web de la institución y el sistema de información de formación de maestros "SIFM" del sistema anual en versión prueba, por lo cual esta muy pocas veces conectado en red. El servidor-3 administra el sistema de registro de alumnos "SIS-INSEA" del sistema semestral y anual, su uso esta limitado a tres usuarios. Mientras que el servidor-2, esta configurado para administrar servicio de internet, el sistema de información de formación de maestros "SIFD" del sistema semestral, el sistema de información contable "SIC-ESFM" y el sistema de registro y control de personal "SRyCP"; el contenido de las base de datos de estos sistemas tiene mucha importancia para la institución y el ministerio de educación, por lo cual acceden todos los usuarios directivos y administrativos.

El equipo tiene las siguientes características:

Fabricante: Intel
Modelo: D848PMB
Nº Serie: MXL7400C86
Microcontrolador: 1.7 GHz
Memoria RAM: 512 MB
Disco Duro: 80 GB (IDE, Marca: Maxtor – S/N: 1234)
Sistema Operativo: Microsoft Windows XP Profesional 2002 con Service Pack 2
Nombre del equipo: SIFD-2012
Dirección IP: 192.168.2.7
Mascara de sub red: 255.255.255.0
Puerta de enlace predeterminada: 192.168.2.1
Antivirus: No
Cortafuegos: No

4.2. Metodología de identificación de vulnerabilidades.

La aplicación de la metodología para identificar vulnerabilidades del servidor-2, se realizo en una iteración, obteniendo los resultados descritos en los siguientes subtítulos.

4.2.1. Prevención de vulnerabilidades.

Las tareas realizadas en esta fase se describen en los siguientes puntos.

4.2.1.1. Evaluación de riesgos.

Esta tarea consistió en predecir el riesgo que evita el perfecto funcionamiento del servidor, también se determino cuáles recursos valen la pena proteger y cuáles son los más importantes. Como primer paso se elaboró una lista de cada uno de los riesgos, luego se efectuó un resumen:

Cuadro N° 4.1

Determinación de riesgos del servidor-2

N°	TIPO DE RIESGO	FACTOR DE RIESGO
1	Virus informático	Muy Alto
2	Accesos no autorizados	Alto
3	Robo de información	Medio
4	Fallas del equipo	Bajo
5	Equivocaciones	Muy Bajo

Fuente: Elaboración propia en base al Cuadro N° 3.1

Indica que habrá que tomar las medidas pertinentes de seguridad para cada riesgo, cuidando incurrir en costos innecesarios según el factor de riesgo.

- Niveles de riesgo de los recursos. Se clasifico de la siguiente manera:

Cuadro N° 4.2

Determinación de la severidad de pérdida de riesgos de los servidores atacados

RECURSO	RIESGO R_n	IMPORTANCIA I_n	RIESGO EVALUADO RR_n
Antena de internet	5	7	35
Switchs	3	8	24
Servidor 1	9	9	81
Servidor 2	10	10	100
Servidor 3	8	9	72
PC's	6	6	36

Es el recurso a proteger más.

Fuente: Elaboración propia en base al Cuadro N° 3.2

La determinación del riesgo general de los recursos obtenido es:

$$RG = \frac{(35 + 24 + 81 + 100 + 72 + 36)}{(7 + 8 + 9 + 10 + 9 + 6)} = 7.1$$

El riesgo total con respecto a los servidores, es de 7 puntos sobre 10, por lo que tenía que buscarse probables causas que pueden provocar problemas a los servicios brindados por los elementos evaluados.

- Identificación de amenazas. Se determino las siguientes medidas preventivas de fallas.

Cuadro N° 4.3

Formulario de registro de amenazas del servidor-2

Objetivo. Listar las amenazas y su efecto en los recursos de los servidores de la organización para conocer las vulnerabilidades.

RECURSO AFECTADO	AMENAZA	VULNERA-BILIDAD	EFECTO
Servidor 2	Falta de Seguridad Física	Tormenta eléctrica	Servidor apagado temporalmente, por lo que se deja de prestar servicios a los demás equipos.
			Daño de algún dispositivo de hardware que puede derivar en la perdida de datos.
		Acceso no Autorizado	Pérdida o robo de dispositivos.
			Robo o alteración de datos, sistemas y aplicaciones.
	Falta de Seguridad Lógica	Virus	Desconfiguración del sistema operativo y pérdida de datos.
			Prestación de servicios de manera interrumpida y lenta.
		Acceso no Autorizado	Robo de información.
			Alteración de datos y sistemas.
	Amenaza en la Red	Agujeros de seguridad en el sistema	Virus.
			Robo de información confidencial.

Fuente: Elaboración propia en base al Cuadro N° 3.3

4.2.1.2. Gestión de vulnerabilidades.

Conocido las amenazas del servidor-2, se realizó las siguientes tareas:

- Actualización y configuración del sistema operativo
- Actualización de aplicaciones y sistemas instalados
- Actualización de usuarios y contraseñas
- Actualización de los antivirus
- Eliminación de aplicaciones, sistemas, programas y archivos

Sin embargo, algunas tareas importantes no se realizaron por falta de presupuesto o falta de aprobación de los responsables de la institución, pero se dio a conocer la importancia que tiene implementar a futuro:

- Utilización de Firewall
- Políticas de seguridad de los servidores

Otra tarea que se realizo es el registro del servidor-2 en formulario; que por ser la primera vez no se tiene datos de gestión de vulnerabilidades, además el administrador desconoce la información por no llevar un registro de puertos, servicios y vulnerabilidades.

Cuadro N° 4.4

Formulario de registro de gestión de vulnerabilidades del servidor-2

Objetivo. Tener información de puertos, servicios, vulnerabilidades y efectos causados a cada uno de los servidores			
DATOS SERVIDOR:			
NOMBRE DEL SERVIDOR:SIFD-2012			
SISTEMA OPERATIVO: Microsoft Windows XP Profesional 2002. Service Pack 2.			
DIRECCIÓN IP: 192.168.2.7		NOMBRE DE DOMINIO:	
MASCARA SUB RED: 255.255.255.0		PUERTA DE ENLACE: 192.168.77.1	
DATOS DE ACTIVIDAD: GESTIÓN DE VULNERABILIDADES			
PUERTO	**PROTOCOLO SERVICIO**	**SERVICIO**	**DETALLE DEL SERVICIO**
---	---	---	---
ID	**VULNERABILIDAD**	**CORRECTIVO**	**EFECTO (ESTADO)**
---	---	---	---

Fuente: Elaboración propia en base al Cuadro N° 3.4

Posteriormente se determino que herramientas se utilizaran en las siguientes fases para detectar las vulnerabilidades del servidor-2.

Cuadro N° 4.5

Formulario de herramientas utilizadas en la identificación de vulnerabilidades del servidor-2

Objetivo: Listar y describir en que se aplicaran las herramientas a utilizar en el análisis forense.	
SOFTWARE	**DESCRIPCIÓN**
VmWareWorkstation 7	Aplicación comercial que permite virtualizar sistemas operativos.
TCPView	Aplicación para detectar puertos abiertos.
Volatility	Conjunto de herramientas desarrolladas en Python para analizar.
Windows XP	Sistema operativo que ha sido atacado. Utilizado en los equipos de trabajo.
Ubuntu Server	Sistema operativo anfitrión donde se aloja el VmWare.
Google	Buscador de información.
Security Focus	Portal web sobre incidentes de seguridad (exploits, soluciones, ataques, etc.)
Microsoft Office	Procesadores de texto, hoja electrónica entre otros para elaborar informe y presentaciones.

Fuente: Elaboración propia en base al Cuadro N° 3.5

4.2.2. Identificación de vulnerabilidades.

La identificación de las vulnerabilidades del servidor consistió en realizar las siguientes tareas:

4.2.2.1. Planificación de vulnerabilidades.

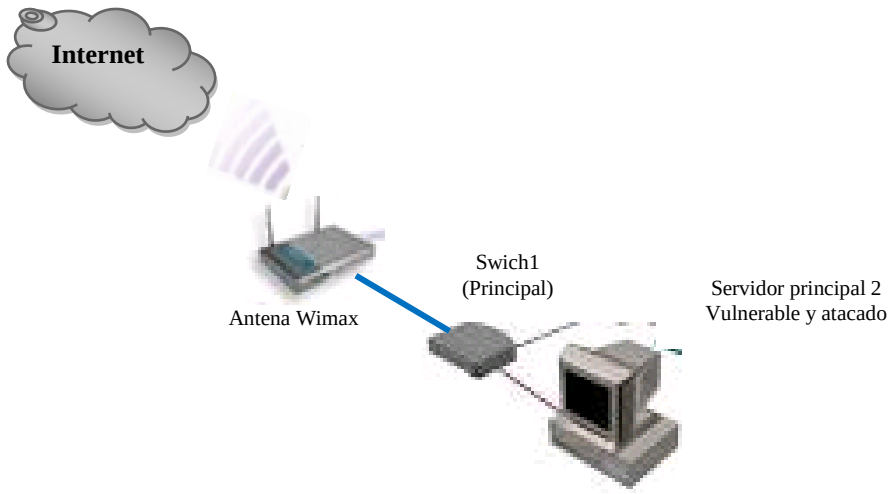
La planificación de vulnerabilidades inicio con la identificación de la infraestructura de red con respecto al servidor: hardware, sistema operativo. Posteriormente se conoció el software, servicios y usuarios, habiendo también programado fecha y hora para desarrollar la identificación de vulnerabilidades en el servidor-2. Los resultados ver en los siguientes formularios:

Cuadro N° 4.6

Formulario de estructura de red con respecto al servidor-2

Objetivo. Conocer los recursos de hardware y software que tiene la organización, lo que permitirá saber información básica de los servidores, el nivel físico de protección y una falla a que servicios o equipos afectara.

ESTRUCTURA DE RED GRÁFICA DE LA ORGANIZACIÓN:



DATOS DE ACTIVIDAD: PLANIFICACIÓN DE VULNERABILIDADES SERVIDOR-2.

SERVIDOR	SISTEMA OPERATIVO	DIRECCION IP	NOMBRE DE DOMINIO	MASCARA DE SUB RED	PUERTA DE ENLACE
SIFD-2012	Microsoft Windows XP Profesional 2002. Service Pack 2.	192.168.2.7	---	255.255.255.0	192.168.77.1

Fuente: Elaboración propia en base al Cuadro N° 3.6

Cuadro N° 4.7

Formulario de registro del servidor-2

<table>
<tr><td colspan="4">Objetivo. Tener una base de conocimiento de los servidores: puertos que utiliza, usuarios y aplicaciones instaladas. Para contar con una bitácora de los servidores de la organización.</td></tr>
<tr><td colspan="4">DATOS SERVIDOR:</td></tr>
<tr><td colspan="4">NOMBRE DEL SERVIDOR:SIFD-2012</td></tr>
<tr><td colspan="4">SISTEMA OPERATIVO: Microsoft Windows XP Profesional 2002. Service Pack 2.</td></tr>
<tr><td colspan="2">DIRECCIÓN IP:192.168.2.7</td><td colspan="2">NOMBRE DE DOMINIO:</td></tr>
<tr><td colspan="2">MASCARA DE SUB RED: 255.255.255.0</td><td colspan="2">PUERTA DE ENLACE: 192.168.77.1</td></tr>
<tr><td colspan="4">DATOS DE ACTIVIDAD: PLANIFICACIÓN DE VULNERABILIDADES</td></tr>
<tr><td colspan="4">FECHA Y HORA PROGRAMA PARA ESCANEO:13-01-2012 horas 12:00 pm</td></tr>
<tr><td colspan="2">DEL:13-01-2012</td><td colspan="2">AL:13-01-2012</td></tr>
<tr><td colspan="2">SOFTWARE</td><td colspan="2">DETALLE DEL SOFTWARE</td></tr>
<tr><td colspan="2">Microsoft Office
Navegadores (Microsoft Internet Explorer, Mozilla Firefox)
Sistemas SIFD, SIC-ESFM, SRyCP</td><td colspan="2"></td></tr>
<tr><td colspan="2">SERVICIO</td><td colspan="2">DETALLE DEL SERVICIO</td></tr>
<tr><td colspan="2">Acceso a base de datos y sistemas: SIFD, SIC-ESFM, SRyCP</td><td colspan="2"></td></tr>
<tr><td>TIPO DE USUARIO</td><td>NOMBRE USUARIO</td><td>USUARIO</td><td>TAREAS/ PROCESOS</td></tr>
<tr><td rowspan="4">Administrador

Cada usuario tiene su computadora y solo inician sesión en la computadora.</td><td>Edilberto…</td><td>Edilberto</td><td>Administración del sistema y base de datos SIFD, SIC-ESFM, SRyCP
Acceso a la base de datos SIFD, SRyCP.</td></tr>
<tr><td>Angel…</td><td>Angel</td><td>Acceso al registro de inscripción del sistema SIFD, SRyCP</td></tr>
<tr><td>Maria…</td><td>Maria</td><td>Acceso al registro de inscripción del sistema SIFD, SRyCP</td></tr>
<tr><td>Orlando…</td><td>Orlando</td><td>Acceso al registro de inscripción del sistema SIFD, SRyCP</td></tr>
<tr><td>PUERTO</td><td>PROTOCOLO</td><td colspan="2">APLICACIÓN/HERRAMIENTA</td></tr>
<tr><td>…</td><td>…</td><td colspan="2">…</td></tr>
</table>

Fuente: Elaboración propia en base al Cuadro N° 3.7

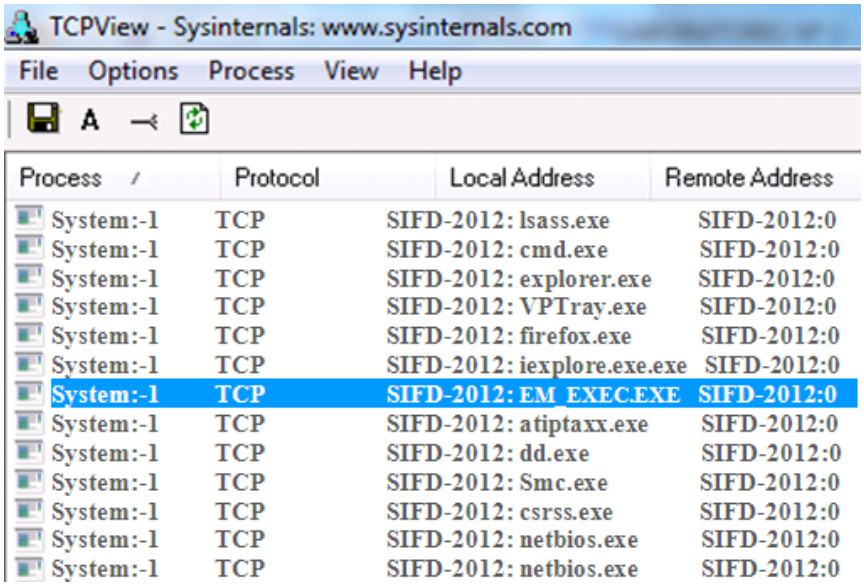
4.2.2.2. Identificación de vulnerabilidades planificadas.

La identificación de vulnerabilidades planificadas con respecto al servidor-2, consistió en:

- Identificación de vulnerabilidades internas. Se utilizó la herramienta TCPView para realizar el escaneo interno y determinar los agujeros de seguridad. Obtenido los siguientes resultados:

Gráfico N° 4.2

Escaneo de puertos abiertos del servidor-2 con TCPView



Fuente: Elaboración propia

Cuadro N° 4.8

Formulario de registro de vulnerabilidades internas del servidor-2

Objetivo. Tener un registro de los resultados obtenidos de la aplicación de las diferentes herramientas utilizadas para el escaneo interno de los servidores.		
DATOS SERVIDOR:		
NOMBRE DEL SERVIDOR: SIFD-2012		
SISTEMA OPERATIVO: Microsoft Windows XP Profesional 2002. Service Pack 2.		
DIRECCIÓN IP: 192.168.2.7	NOMBRE DE DOMINIO:	
MASCARA DE SUB RED: 255.255.255.0	PUERTA DE ENLACE: 192.168.77.1	
DATOS DE ACTIVIDAD: IDENTIFICACIÓN DE VULNERABILIDADES INTERNAS		
ID	**HERRAMIENTA**	**VULNERABILIDAD**
1	TCPView	Puertos abiertos

Fuente: Elaboración propia en base al Cuadro N° 3.8

4.2.2.3. Análisis de vulnerabilidades.

Realizado un análisis al resultado de vulnerabilidad interna, y verificado en el servidor-2, se confirma que si existe tal vulnerabilidad, por lo que se mantiene la lista.

Cuadro N° 4.9

Formulario de registro de análisis de vulnerabilidades del servidor-2

Objetivo. Conocer el análisis realizado a cada una de las vulnerabilidades listadas por las herramientas, para desechar aquellas falsas vulnerabilidades.			
DATOS SERVIDOR:			
NOMBRE DEL SERVIDOR:SIFD-2012			
SISTEMA OPERATIVO: Microsoft Windows XP Profesional 2002. Service Pack 2.			
DIRECCIÓN IP:192.168.2.7		NOMBRE DE DOMINIO:	
MASCARA DE SUB RED: 255.255.255.0		PUERTA DE ENLACE: 192.168.77.1	
DATOS DE ACTIVIDAD: IDENTIFICACIÓN DE VULNERABILIDADES INTERNAS			
ID	**HERRAMIENTA**	**VULNERABILIDAD**	**OBSERVACION (ANÁLISIS)**
1	TCPView	Puertos abiertos	

Fuente: Elaboración propia en base al Cuadro N° 3.10

4.2.2.4. Búsqueda y verificación de vulnerabilidades reales.

Nuevamente la información detectada como vulnerabilidad real fue escaneada, llegando a los mismos resultados. Obteniendo el siguiente registro.

Cuadro N° 4.10

Formulario de registro de búsqueda y verificación de vulnerabilidades reales del servidor-2

Objetivo. Tener un registro de la búsqueda y verificación de cada vulnerabilidad real para cada servidor.		
DATOS SERVIDOR:		
NOMBRE DEL SERVIDOR:SIFD-2012		
SISTEMA OPERATIVO: Microsoft Windows XP Profesional 2002. Service Pack 2.		
DIRECCIÓN IP:192.168.2.7	NOMBRE DE DOMINIO:	
MASCARA DE SUB RED: 255.255.255.0	PUERTA DE ENLACE: 192.168.77.1	
DATOS DE ACTIVIDAD: BÚSQUEDA Y VERIFICACIÓN DE VULNERABILIDAD REALES.		
FECHA:13-01-2012		
DETALLE DEL SERVICIO	**SERVICIO**	**PUERTO**
Acceso con: ▪ Mozilla Firefox ▪ Microsoft Internet Explorer	Internet	1055, 1056 1077, 1082, 1066
ID	**VULNERABILIDAD**	**ESTADO**
1	Puerto Abierto	…

Fuente: Elaboración propia en base al Cuadro N° 3.11

4.2.3. Corrección de vulnerabilidades.

Verificado las vulnerabilidades reales en el servidor-2, se realizo la corrección mediante la búsqueda de correctivos.

4.2.3.1. Búsqueda de correctivos.

Para corregir la vulnerabilidad del servidor-2 se procedió con la búsqueda de correctivos, habiendo registrado lo siguiente:

Cuadro N° 4.11

Formulario de registro de la corrección de vulnerabilidades del servidor-2

Objetivo. Tener una bitácora de los escaneos de vulnerabilidades y de la correcta atención a cada vulnerabilidad encontrada.			
DATOS SERVIDOR:			
NOMBRE DEL SERVIDOR:SIFD-2012			
SISTEMA OPERATIVO: Microsoft Windows XP Profesional 2002. Service Pack 2.			
DIRECCIÓN IP:192.168.2.7		NOMBRE DE DOMINIO:	
MASCARA DE SUB RED: 255.255.255.0		PUERTA DE ENLACE: 192.168.77.1	
DATOS DE ACTIVIDAD: BÚSQUEDA Y VERIFICACIÓN DE VULNERABILIDAD REALES.			
FECHA:17-01-20012			
PUERTO	**PROTOCOLO SERVICIO**	**SERVICIO**	**DETALLE DEL SERVICIO**
1055, 1056 1077, 1082, 1066	TCP/IP	Internet	Acceso: Mozilla Firefox Microsoft Explorer
ID	**VULNERABILIDAD**	**CORRECTIVO**	**EFECTO (ESTADO)**
1	Puerto Abierto	Cierre del puerto con regedit	Puerto cerrado

Fuente: Elaboración propia en base al Cuadro N° 3.12

4.2.3.2. Informe final y presentación de la información.

Como se menciono en anterior capítulo, es la fase final de la investigación, aquí se presentan resultados de la identificación de vulnerabilidades. Este informe no fue desarrollado por su amplitud, además que el objetivo del capitulo es seguir los pasos de la metodología propuesta. Sin embargo, se recomienda mantener como contenido mínimo lo sugerido en el capítulo anterior.

4.3. Metodología de análisis forense.

La aplicación de la metodología de análisis forense en el servidor-2, se resolvió en una iteración, habiendo obtenido el siguiente resultado que se muestra a manera resumida.

4.3.1. Identificación de la evidencia.

En esta fase se identifico las evidencias del servidor.

4.3.1.1. Solicitud forense.

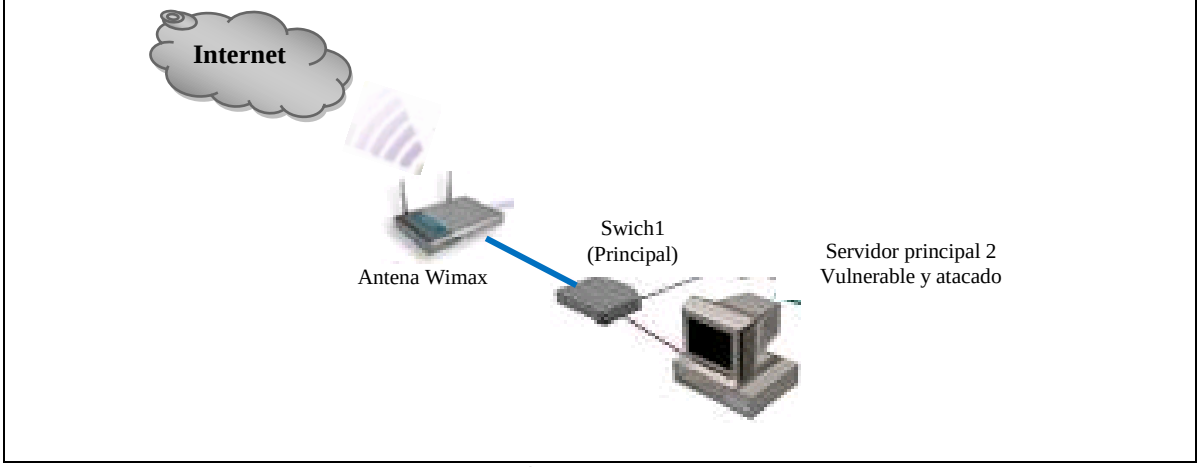
El administrador del servidor-2 notifico la ejecución de un incidente, solicitando con la aprobación de la parte directiva, la revisión mediante el llenado del siguiente formulario:

Cuadro N° 4.12

Formulario de solicitud forense del servidor-2

Objetivo.La presente solicitud describe toda la información del incidente ocurrido con el servidor de la organización.
1. DESCRIPCIÓN DEL DELITO INFORMÁTICO.
Fecha del incidente:*16-01-2012* Duración del incidente (si se puede establecer): Detalles del incidente: S*ervidor-2, bajo rendimiento en la velocidad de arranque y ejecución del sistema, aplicaciones u archivos. Las bases de datos no responden en su ejecución.* Como se descubrió el incidente: *Al iniciar el equipo, este no respondía solo reiniciaba* Otros aspectos que se consideren importantes en el incidente, describir:
2. INFORMACIÓN GENERAL.
Área: *Unidad de Informática* Nombre de la dependencia: *Min. Educ*. **Responsable servidor (sistema afectado):** Nombres y Apellidos: *Edilberto* Cargo: *Técnico III Responsable Sistemas* E-mail:*edilb_esfmea@gmail.com* Teléfono: Celular: *72447035* Si sabe de otro equipo o sistema que haya sufrido el mismo problema o uno similar: *Los servidores 1 y 3, además de algunas computadoras clientes.*
3. INFORMACIÓN DEL SERVIDOR (EQUIPO AFECTADO).
Nombre del servidor: SIFD-2012 Dirección IP: 192.168.2.7 Marca: Modelo: Capacidad de la RAM:Capacidad del disco duro: Modelo del Procesador: Sistema operativo (nombre y versión): Microsoft Windows XP Profesional 2002 con Service Pack 2 Función del equipo: *Almacena información de los alumnos con respecto a inscripciones, calificaciones, datos de los docentes y administrativos hasta la gestión2012, entre otros.* Tipo de información procesada por el servidor: *Bases de datos de inscripciones, calificaciones, datos de docentes y administrativos.* Usuarios:*Administrador del servidor, técnicos de archivos y kardex (3 personas)* Servicios: *Consulta y registro de información en el sistema SIFD-2012* Observaciones:

4. ESTRUCTURA DE RED GRÁFICA DE LA ORGANIZACIÓN CON RESPECTO AL SERVIDOR:



Fuente: Elaboración propia en base al Cuadro N° 3.14

4.3.1.2. Asegurar la escena.

En esta tarea se trabajo de forma metódica, cuidando de no perder huellas del servidor-2 que es la evidencia por lo que se preservó en su estado original protegiendo su entorno. Este se encontraba encendido, se cuido que no sea apagado por otro tipo de incidente; es decir, se despejo el área asegurando que nadie tenga acceso a la computadora o sus alrededores para no perder huellas, solo se procedió a ver las pantallas que se encontraban abiertas incluyendo el sistema operativo. Se protegió con cinta de evidencia los lectores, disqueteras y se rotulo la evidencia con los siguientes datos:

Cuadro N° 4.13

Formulario de rotulo de evidencias del servidor-2

Objetivo: Registrar información de la evidencia encontrada	
N°	1
CASO	Servidor-2 ESFM EA - 2012
FECHA	16-01-2012
HORA	16:47:50
TIPO	Computadora servidor
OBSERVACIONES	Servidor 2 con probable infección de virus.
FIRMA	

Fuente: Elaboración propia en base al Cuadro N° 3.15

4.3.1.3. Identificar las evidencias.

Con el fin de determinar las evidencias y orden de prioridad de los incidentes, se realizo todos los procesos necesarios para detectar los incidentes, logrando el siguiente resultado:

Cuadro N° 4.14

Formulario de daños producidos y recursos afectados al servidor-2

Objetivo: Tener información de los efectos del incidente y recursos afectados al servidor.						
INCIDENTE	**EXTENSIÓN DE DAÑOS PRODUCIDOS**			**CRITICIDAD DE LOS RECURSOS AFECTADOS**		
	GRAVE	**MODERADO**	**LEVE**	**ALTA**	**MEDIA**	**BAJA**
Infección de virus						
Servidor-1		x			x	
Servidor-2	X			x		
Servidor-3		x			x	
Acceso no autorizado						
Servidor-1		x			x	
Servidor-2	X				x	
Servidor-3		x				x

Fuente: Elaboración propia en base al Cuadro N° 3.16

Cuadro N° 4.15

Formulario de criticidad de los daños producidos al servidor-2

Objetivo: Tener información de la criticidad de los daños del servidor por efecto de un incidente que causo daños y afecto recursos. Además de obtener la prioridad de los incidentes según el administrador.		
INCIDENTE	**CRITICIDAD DE LOS DAÑOS**	**PRIORIDAD**
Infección de virus servidor-2	Muy Grave	10
Acceso no autorizado servidor-2	Grave	7
Infección de virus servidor-3	Moderado	4
Acceso no autorizado servidor-1	Moderado	4
Infección de virus servidor-1	Moderado	4
Acceso no autorizado servidor-3	Leve	1

Fuente: Elaboración propia en base al Cuadro N° 3.17

Al ser atacado el servidor-2 se constituyo en una evidencia; los resultados muestran que el incidente “infección de virus servidor-2” es el que requería mayor prioridad. Con esta información se identificó aquellos dispositivos que son evidencia: los discos duros, un flash que estaba insertado en el servidor, la memoria RAM porque la computadora estaba encendida, el sistema operativo, aplicaciones y otros sistemas de la institución. Con esta información se determino el proceso a seguir para recuperar evidencia y las herramientas a utilizar.

4.3.2. Preservación de la evidencia.

Con la información recabada se definió el procedimiento a seguir para el almacenamiento y etiquetado de las evidencias, también se determino las herramientas a utilizar:

Cuadro N° 4.16

Formulario de herramientas utilizadas en el análisis forense del servidor-2

Objetivo: Listar y describir en que se aplicaran las herramientas a utilizar en el análisis forense.	
SOFTWARE	**DESCRIPCIÓN**
VmWareWorkstation	Aplicación comercial que permite virtualizar sistemas operativos.
Volatility	Conjunto de herramientas desarrolladas en Python para analizar capturas de memoria RAM.
Windows XP	Sistema operativo que ha sido atacado. Utilizado en los equipos de trabajo.
Ubuntu Server	Sistema operativo anfitrión donde se aloja el VmWare.
Google	Buscador de información.
CritoRes	Programa matemático para obtener la función hash MD5, SHA-1
Microsoft Office	Procesadores de texto, hoja electrónica entre otros para elaborar informe y presentaciones.
Whois	Es un servidor que almacena toda la información de un conjunto de dominios o IP's (con lo que ese servidor es capaz de responder a cualquier consulta de dominios).

Fuente: Elaboración propia en base al Cuadro N° 3.18

4.3.2.1. Copias de la evidencia.

El servidor-2 se encontraba encendido, por lo que se procedió a sacar una imagen[9] (copia) de la memoria RAM utilizando la herramienta volatility, obteniendo como resultado la imagen:



xp-pcservidor-2012-01-16.img

Posteriormente se realizo otra copia de la imagen obtenida, luego se generó una suma de comprobación de la integridad de las copias utilizando la función hash MD5, seguidamente se colocaron etiquetas de evidencia original (fecha, hora extracción). También se realizo copias de los discos duros y memoria usb (pendrive) que estaba insertado en el servidor. En resumen, se trato de obtener el mayor numero de evidencias para cuando se presente el caso a las autoridades competentes, se tendrían las suficientes pruebas que certifiquen y aseveran los hallazgos. Un resumen de las pruebas identificadas que se llevaron a laboratorio para hacer el análisis forense y la correcta recolección de la información es la siguiente:

[9]Imagen forense: es crear una copia exacta del dispositivo o equipo original en uno nuevo mediante técnicas y herramientas. Esto significa que el original y la copia son idénticos, al grado que de ambas se pueda recuperar información borrada a través de técnicas.

Cuadro N° 4.17

Formulario de control de copias de evidencias del servidor-2

Objetivo: Mencionar actividades de copias de evidencia que se realizaron.			
ACTIVIDAD	**SI**	**NO**	**OBSERVACIÓN**
Imagen de la memoria RAM de bit a bit	x		
Generar autenticación matemática de los datos a través del algoritmo de hash	x		
Etiquetar evidencia, registro de fecha y hora del sistema	x		
Generar una lista de palabras claves a buscar	x		

Fuente: Elaboración propia en base al Cuadro N° 3.19

4.3.2.2. Cadena de custodia.

La evidencia (servidor-2) se movió a un lugar seguro dentro de la unidad de informática de la institución, fuera del alcance de los usuarios, cuidando de no colocar ningún elemento electromagnético cerca, con las recomendaciones respectivas de su importancia al responsable, quedando registrada de la siguiente manera:

Cuadro N° 4.18

Formulario de cadena de custodia del servidor-2

Objetivo: Describir la ubicación de la evidencia y su traslado.					
N°	**UBICACIÓN ACTUAL**	**FECHA**	**RAZON DE TRASLADO**	**SITIO A DONDE SE TRASLADA**	**OBSERVACIONES (quién, sus datos)**
1	Al ingreso de la puerta unidad de informática de la institución	16-01-2012	Incidente	A un extremo de la misma unidad cubierto por mamparas.	Responsable Edilberto.
LUGAR DE DEPÓSITO FINAL DE LA EVIDENCIA: A un extremo de la misma unidad cubierto por mamparas.					**FECHA:** 16-01-2012

Fuente: Elaboración propia en base al Cuadro N° 3.20

4.3.3. Análisis de la evidencia.

En esta fase se trabajo con una visión técnica, cuidando que los datos del archivo no cambien al ser muy relevante en un proceso judicial. Sin embargo, por la cantidad de evidencia recolectada que implica un extenso trabajo de análisis forense, se analizo solo el archivo de imagen, obteniendo los resultados descritos en los siguientes subtítulos.

4.3.3.1. Preparación para el análisis.

La preparación consistió en determinar y preparar la maquina a utilizar para el análisis del archivo de imagen, con las siguientes características:

Sistema operativo “Windows 7 Home Premium”

Microcontrolador: Intel (R) Core (TM) 2 Duo CPU 3 GHz

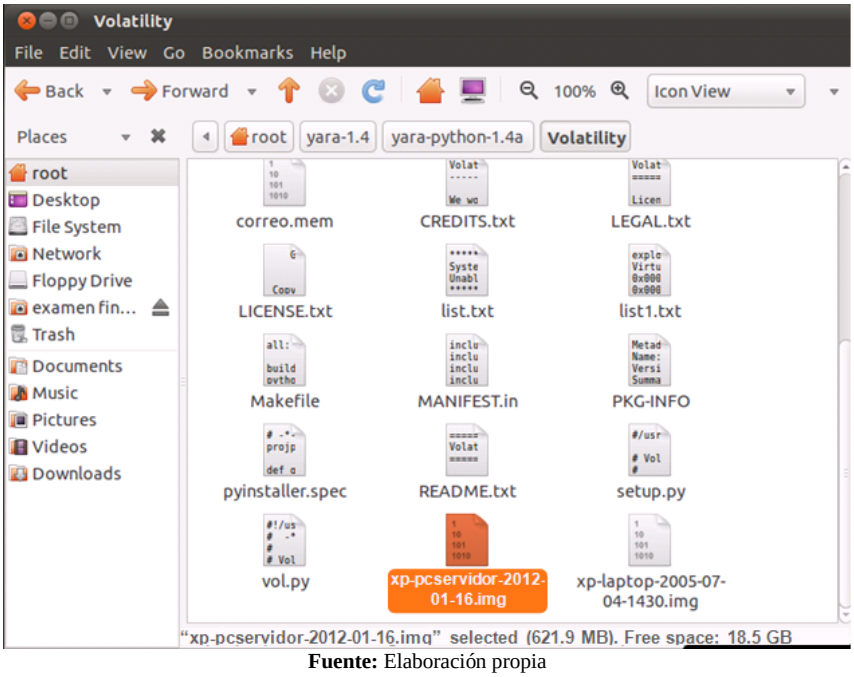
Memoria RAM: 2 GHz

Disco Duro: 360 GB (IDE – MARCA: Maxtor)

A este equipo se instaló una maquina virtual “VMWARE Workstation 7”, con el sistema operativo “Linux Ubuntu 10.10”. Posteriormente se instalo la utilidad “Volatility” para analizar las capturas de memoria RAM, a cuyo directorio se movió la imagen de memoria proporcionada.

Gráfico N° 4.3

Imagen del servidor-2 movido a la herramienta Volatility



Fuente: Elaboración propia

4.3.3.2. Reconstrucción de la secuencia temporal del ataque.

Montadas las imágenes del sistema atacado, se procedió a reconstruir la secuencia temporal del ataque:

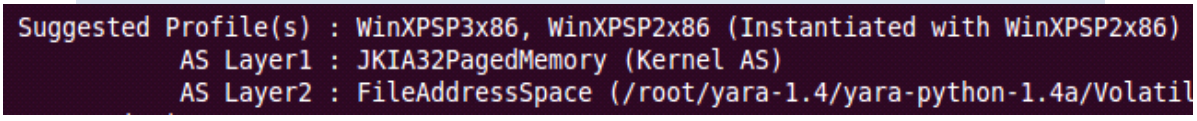
- Identificación de imagen. Con la imagen se realizo una comprobación matemática de la función hash (MD5) para verificar la originalidad.

- Características del sistema operativo. A partir de esta tarea se utilizo la herramienta Volatility para determinar el sistema operativo de la imagen de memoria, con lo que se realizo el siguiente análisis: el perfil sugerido o recomendado para continuar con el análisis es Windows con Service Pack 2 (WinXPSP2x86).

Gráfico N° 4.4

Sistema operativo del servidor-2 obtenido a partir de la imagen

Instrucción ejecutada: python vol.py -f xp-pcservidor-2012-01-16.img imageinfo



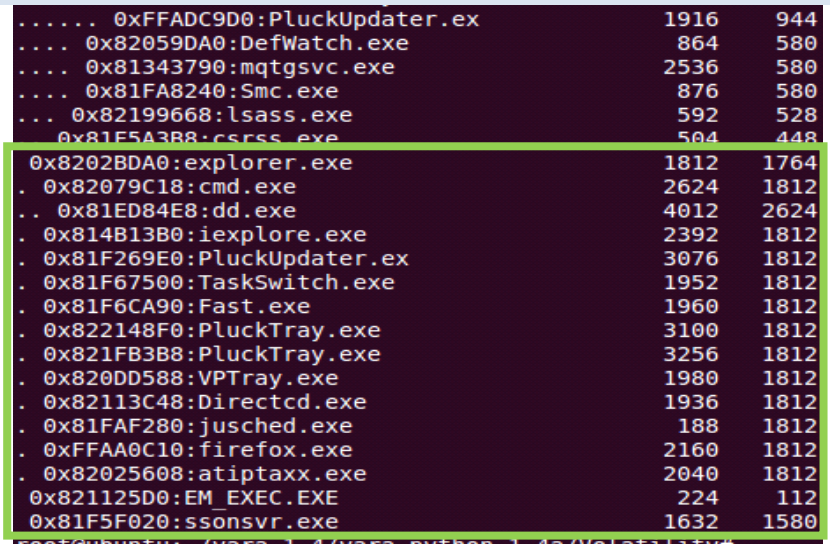
Fuente: Elaboración propia

- Procesos y Servicios en ejecución. Primeramente se indago en los procesos que se ejecutaron, posteriormente los servicios que se encontraban en ejecución.

Gráfico N° 4.5

Resumen de procesos ejecutados del servidor-2 obtenido a partir de la imagen

Instrucción ejecutada:
python vol.py –profile = WinXPSP2x86 -f xp-pcservidor-2012-01-16.img pstree



Fuente: Elaboración propia

Al observar el gráfico anterior, desde el proceso explorer.exe se tiene algunos procesos que no son iniciados por el sistema, sino por el usuario o por la instalación de algún programa que realizo el mismo usuario. Por lo que se indago en los siguientes procesos que son archivos ejecutables:

- explorer.exe (pid 1812). Proceso básico de Windows que administra la interfaz del usuario (intérprete de comandos) y también la interfaz gráfica de Windows (escritorio).
- cmd.exe (pid 2624.exe). Proceso genérico de Windows que abre una consola de modo texto para ejecutar programas utilizando una línea de comando. Su proceso padre: explorer.exe
- dd.exe (pid 4012). Proceso que pertenece al programa desconocido del fabricante desconocido, permite editar fotos y encargar copias, álbumes, etc. Cuando provoca errores en Windows, puede deberse a que el registro contenga entradas dañadas o se ha producido una infección por virus. Su proceso padre: cmd.exe
- iexplore.exe (pid 2392). Proceso principal y responsable del programa Microsoft Internet Explorer. Esta aplicación permite al usuario navegar por Internet o conectarse a intranets. Su proceso padre: explorer.exe
- firefox.exe (pid 2160). Proceso del navegador web de internet "Mozilla Firefox". Su proceso padre: explorer.exe
- EM_EXEC.EXE (pid 224). Proceso de sistema instalado con el Logitech MouseWare, algunos malware se camuflan con este nombre.

Con esta información se confirmo que en el momento del incidente se utilizaba el servicio de internet.

4.3.3.3. Determinación de cómo se realizó el ataque.

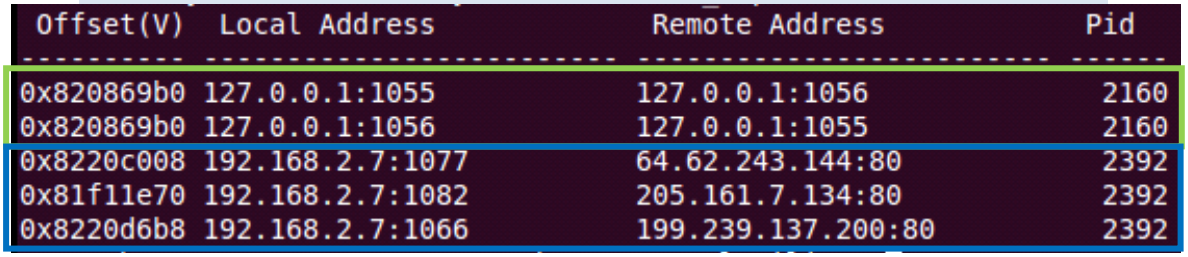
Para analizar cómo ocurrió el ataque, se verifico de cada proceso las conexiones de red, tal como se describe:

- Trabajos en red. La información recabada sobre los PID (identificador de un proceso): iexplore.exe (pid: 2392) y firefox.exe (pid: 2160), permitió determinar las conexiones de puertos que se encontraban abiertos.

Gráfico N° 4.6

Conexiones de puertos abiertos del servidor-2 obtenido a partir de la imagen

Instrucción ejecutada: python vol.py -f xp-laptop-2005-06-25.img connections



Offset(V)	Local Address	Remote Address	Pid
0x820869b0	127.0.0.1:1055	127.0.0.1:1056	2160
0x820869b0	127.0.0.1:1056	127.0.0.1:1055	2160
0x8220c008	192.168.2.7:1077	64.62.243.144:80	2392
0x81f11e70	192.168.2.7:1082	205.161.7.134:80	2392
0x8220d6b8	192.168.2.7:1066	199.239.137.200:80	2392

Fuente: Elaboración propia

- Huellas de la intrusión. Obtenido la información del uso de internet con los navegadores Internet Explorer (iexplore.exe) Mozilla Firefox (firefox.exe), puertos abiertos (1077, 1082 y 1066) y direcciones de red a la que se accedió remotamente, se identifico que los accesos al servidor fueron desde las direcciones IP: 205.161.7.134 Puerto: 80, IP: 199.239.137.200 Puerto: 80 y IP: 64.62.243.144 Puerto: 80. A esto se suma que se tenía un archivo EM_EXEC.EXE en ejecución en fecha 16-01-2012 horas 16:51:02.

4.3.3.4. Identificación del atacante.

Identificado los procesos sospechosos y sus direcciones, se verifico el origen del ataque con la ayuda de la página web WHOIS, obteniendo el siguiente resultado:

- La IP: 199.239.137.200 es una dirección web que tiene asignado dos sitios (nytoday.com y nythontheweb.com) alojados en servidores de Estados Unidos.
- Las direcciones IP: 205.161.7.134 y IP: 64.62.243.144 no son direcciones web, son direcciones de servidores ubicados en un Estados Unidos, sus ultimas actualizaciones fueron el 25 de mayo del 2011.

4.3.3.5. Perfil del atacante.

Por la información recabada se determino que el atacante es un SciptKiddies que ingreso de manera no autorizada al servidor-2, utilizando IP prestadas (IP: 205.161.7.134 IP:

64.62.243.144) para modificar el archivo EM_EXEC.EXE, convirtiéndolo en un archivo infectado por virus, el cual fue detectado por el antivirus del servidor, pero no fue desinfectado.

4.3.3.6. Evaluación del impacto causado al sistema.

El servidor-2 quedo inhabilitado por bajo rendimiento en la velocidad de ejecución y respuesta hacia los demás equipos de la red. Además, la base de datos del sistema SIFD-2012 y el mismo sistema quedo desconfigurada.

4.3.4. Documentación y presentación de pruebas.

Como se menciono en anterior capítulo, es la fase final de la investigación, aquí se presentan resultados y hallazgos en dos tipos de informes: técnico y ejecutivo. Estos informes no fueron desarrollados por su amplitud, además el objetivo del capitulo fue seguir las fases de la metodología propuesta. Sin embargo, se recomienda mantener como contenido mínimo los títulos y subtítulos mencionados en capítulo anterior.

4.3. Viabilidad de la metodología propuesta mediante el criterio de expertos.

Con la finalidad de validar la propuesta metodológica “metodología de identificación de vulnerabilidades y análisis forense para servidores de una organización”, se acudió al criterio de especialistas, quienes han sido seleccionados por su conocimiento sobre el tema de estudio al haberse dedicado a la investigación y por su experiencia profesional.

Para la selección de los expertos se recurrió al método estadístico no probabilístico “Muestreo de selección experta”, teniendo como población a profesionales especialistas en el tema que cumplen los requisitos establecidos, de los cuales mediante el criterio de idoneidad, objetividad y predisposición 7 especialistas fueron seleccionados como muestra poblacional.

4.4.1. Procesamiento de las encuestas a través del método Delphy.

Para viabilizar la metodología se utilizo el método de expertos Delphy, mediante el cual se elaboró el contenido del cuestionario (ver en Anexo Nº 11), luego se aplicó la consulta de opiniones al grupo de especialistas seleccionados con el fin de valorar su coeficiente de competencia y someter a su criterio la metodología propuesta para conocer su valoración sobre la viabilidad de la metodología propuesta y obtener su aprobación.

4.4.2. Análisis a los resultados del criterio de expertos.

Todas las recomendaciones realizadas por los especialistas permitieron perfeccionar la metodología propuesta, así como su aplicación practica, cuyas modificaciones finales están contenidas en este informe final. Como conclusión de estas correcciones y resultados de la encuesta aplicada a los especialistas (ver en Anexo Nº 12), el trabajo quedo apto para su presentación y se tiene la aprobación de los especialistas que calificaron el objetivo de la tesis, los capítulos II y III bastante adecuado, mientras que el capítulo IV como adecuado.

Por tanto, se considera que la metodología de identificación de vulnerabilidades y análisis forense para servidores de una organización, esta en función de satisfacer las necesidades de administradores de servidores y especialistas forenses, lo que posibilita mejorar la seguridad de los servidores, dando así solución al problema planteado y cumplimiento de los objetivos propuestos.

CONCLUSIONES

- Se contribuye con una metodología abierta a la que cualquier persona entendida en el área puede acceder, estudiar en sus partes, ampliar, sugerir y contribuir. Donde todas las críticas constructivas ayudaran a la evolución de esta metodología; todo con el fin de contribuir a la disciplina de la seguridad informática.

- Para lograr el éxito de la implementación de la metodología propuesta, es necesario que el administrador se comprometa a seguir la metodología de tal forma que se facilite la evaluación y aprobación de resultados e implementación de planes de difusión dentro de la institución, con la finalidad de garantizar la seguridad en el manejo de la información.

- Los resultados de la aplicación de la metodología propuesta proveen información sobre las debilidades, vulnerabilidades y/o actos ilegales que posee una organización, siendo este el punto de partida para la toma de decisiones en relación a la seguridad informática dentro de la institución, con el fin de garantizar un aseguramiento y funcionamiento exitoso de los servidores.

- La aplicación de la metodología propuesta a los servidores de una institución educativa ESFM EA, radicó en la falta de seguridad, el desconocimiento de la importancia que ésta tiene dentro de la institución, la inexistencia de métodos o procesos formales aplicados a la identificación de vulnerabilidades y análisis forense.

- La metodología desarrollada para la identificación de vulnerabilidades proporciona alternativas suficientes y necesarias para proteger e identificar los recursos críticos y dar solución a los problemas de intrusión y amenazas, así como el de solucionar la problemática de los usuarios finales en el manejo de información y servicios del servidor.

- Con la metodología propuesta para realizar análisis forense, se concluye que es inevitable la necesidad de buscar amenazas, evidencias y causas, cuando el servidor de una organización está comprometido en un crimen informático. Su aplicación permite determinar las causas y dar solución garantizando la seguridad en una organización.

RECOMENDACIONES

- Se recomienda utilizar herramientas de identificación de vulnerabilidades y análisis de evidencias, que cuente con un soporte adecuado de su fabricante y con una base de datos muy completa, y que en lo posible sea una herramienta automatizada para mejorar la efectividad del proceso.

- Ante actos de intrusión, se recomienda a los responsables de servidores, realizar un análisis profundo de los hallazgos encontrados con la aplicación de la metodología propuesta;para obtener resultados exactos y válidos legalmente.

- Por el avance tecnológico y cambios en las leyes bolivianas, la metodología debe ser actualizada a todos los segmentos de la red, teniendo en cuenta los cambios que incluyan los recursos de hardware y software de las computadoras; debido a que son recursos manejados por los usuarios y mucha de la información almacenada es crítica, además de garantizar más aun la seguridad de los servidores y evitarse cualquier tipo de problemas.

- Aplicada la metodología y obtenido los resultados de la institución educativa ESFM EA, se recomienda a los responsables de la institución implementar continuamente métodos y políticas de seguridad informática enfocadas al usuario final y amenazas de intrusos, como la utilización de un cortafuego (firewall) para bloquear el acceso no autorizado y permitir al mismo tiempo comunicaciones autorizadas, además de crear e implementar políticas de seguridad para los servidores de la red (accesos, usuarios, etc.).

- Para la aplicación de la metodología propuesta se recomienda mantenerse informado de las nuevas herramientas de seguridad disponible según el sistema operativo del servidor, debido a que las amenazas y como consecuencia las vulnerabilidades cada día aumentan y cambian rápidamente.

BIBLIOGRAFÍA

Libros impresos:

Básica

HERZOG, P. *Manual de la Metodología Abierta de Testeo de Seguridad OSSTMM 3.0.* 4a ed. New York- EE.UU.: Editorial ISECOM Institute For Security and Open Methodologies, 2010.

TORI, C. *Hacking Ético.* Argentina: Carlos Tori, 2008.

Metodológica

DEL CANTO, C. *Programa de Maestría en Educación Superior.* La Habana: UCP EJV, 2010.

HERNANDEZ, R.; FERNANDEZ, C. Y BAPTISTA, P. *Metodología de la Investigación.* 2a ed. México: McGraw-Hill, 1998.

LOZANO, G. *Metodología de la Investigación y Asesoría de Tesis*. Lima: Editorial Instituto de Investigación Docencia, 2010.

TAMAYO, M. *El Proceso de la Investigación Científica*. 2a ed. México: Editorial Limusa, 1991.

TORRES, P. *¿Cómo Redactar una Tesis?.* Potosí: A. B. (Asesores Bioestadísticos), 1997.

ZORRILLA, S. y TORRES, M. *Guía para Elaborar la Tesis*. 3a ed. México: McGraw-Hill, 2000.

Libros electrónicos:

BELLO, C. *Manual de seguridad en redes* [en línea]. Argentina: Editor ArCert. 2011. Disponible en: http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf.

FERRER, F. *Servidores Windows* [en línea]. 3ª ed. España: Creative Commos. 2009. Disponible en: http://www.etnassoft.com/biblioteca/servidores-windows/.

FUENTES, S. *Defiende tu PC. Guía de Seguridad Para Ordenadores Personales* [en línea]. Barcelona: Gatex Quality S.L. 2005. Disponible en: http://spamloco.net/2006/08/defiende-tu-pc-gua-de-seguridad-para.html.

HERNANDEZ, C. *Hackers. Los piratas del Chip y de Internet* [en línea]. Argentina: Claudio Hernández. 2001. Disponible en: http://perso.wanadoo.es/snickers/.

LOPEZ, M. *Análisis Forense Digital* [en línea]. 2a ed. México: Hackers & Seguridad. 2007. Disponible en: http://oas.org/juridico/spanish/cyb_analisis_foren.pdf.

Trabajos de titulación:

ALMEIDA, O. *Metodología para la Implementación de Informática Forense en Sistemas Operativos Windows y Linux.* Trabajo de titulación (Ingeniero en Sistemas Computacionales). Ibarra-Ecuador: Universidad Técnica del Norte, 2011. 151p.

BORGHELLO, C. *Seguridad Informática sus Implicancias e Implementación*. Trabajo de titulación (Licenciatura en Sistemas). Argentina: Universidad Tecnológica Nacional, 2007. 278 p.

PALLAS, G. *Metodología de Implantación de un SGSI en un grupo empresarial jerárquico*. Trabajo de titulación (Maestría en Ingeniería en Computación). Montevideo-Uruguay: Ingeniería, Universidad de la República, 2009. 186p.

VALDESPINO, A. *Propuesta de una metodología de análisis forense para PDA (Asistentes Personales Digitales).* Trabajo de titulación (Maestro en Ciencias de Ingeniería en Microelectrónica). México: Instituto Politécnico Nacional, 2009. 58p.

Página web institucional:

Círculo de Deming. Editor Wikipedia. Disponible en: http://es.wikipedia.org/wiki/C%C3%ADrculo_de_Deming. Fecha de consulta 3 de Septiembre del 2012.

Conceptos básicos sobre ISO 27001. Editor IS&BCA. Disponible en: http://www.iso27001standard.com/es/que-es-la-norma-iso-27001#documentos. Fecha de consulta 2 de Septiembre del 2012.

Gestión de Incidentes – Análisis Forense. Editor IBM Corporation. Disponible en: http://www.asiap.org/AsIAP/images/stories/JIAP/jiap2011/Presentaciones/Azul/A1715_IBM.pdf. Fecha de consulta 15 de Febrero del 2012.

Las 75 Herramientas de Seguridad Más Usadas. Editor ThiOsk. Disponible en: http://insecure.org/. Fecha de consulta 20 de Febrero del 2012.

Los Sherlock Holmes Modernos. Editor Magazine Premium. Disponible en: http://www.magazcitum.com.mx/?p=24. Fecha de consulta 15 de Septiembre del 2012.

Metodología de Análisis Forense. Editor UTN – FICA – EISIC. Disponible en: http://repositorio.utn.edu.ec/bitstream/123456789/539/21/04%20ISC%20157%20RESUMEN%20TECNICO%20ESPA%C3%91OL.pdf. Fecha de consulta 10 de Diciembre del 2011.

Portal de Soluciones Técnicas y Organizativas a los Controles de ISO/IEC 27002. Editor ISO. Disponible en: http://iso27002.wiki.zoho.com/. Fecha de consulta 20 de Septiembre del 2012.

REFERENCIAS BIBLIOGRÁFICAS

HERZOG, P. *Manual de la Metodología Abierta de Testeo de Seguridad OSSTMM 3.0.* 4a ed. New York- EE.UU.: Editorial ISECOM Institute For Security and Open Methodologies, 2010.

PALLAS, G. *Metodología de Implantación de un SGSI en un grupo empresarial jerárquico*. Trabajo de titulación (Maestría en Ingeniería en Computación). Montevideo-Uruguay: Ingeniería, Universidad de la República, 2009. 186p.

HERZOG, P. *Op. cit.*

HERZOG, P. *Op. cit.*

Los Sherlock Holmes Modernos. Editor Magazine Premium. Disponible en: http://www.magazcitum.com.mx/?p=24. Fecha de consulta 15 de Septiembre del 2012.

ALMEIDA, O. *Metodología para la Implementación de Informática Forense en Sistemas Operativos Windows y Linux.* Trabajo de titulación (Ingeniero en Sistemas Computacionales). Ibarra-Ecuador: Universidad Técnica del Norte, 2011. 151p.

ALMEIDA, O. *Op. cit.*

Conceptos básicos sobre ISO 27001. Editor IS&BCA. Disponible en: http://www.iso27001standard.com/es/que-es-la-norma-iso-27001#documentos. Fecha de consulta 2 de Septiembre del 2012.

Círculo de Deming. Editor Wikipedia. Disponible en: http://es.wikipedia.org/wiki/C%C3%ADrculo_de_Deming. Fecha de consulta 3 de Septiembre del 2012.

Portal de Soluciones Técnicas y Organizativas a los Controles de ISO/IEC 27002. Editor ISO. Disponible en: http://iso27002.wiki.zoho.com/. Fecha de consulta 20 de Septiembre del 2012.

BORGHELLO, C. *Seguridad Informática sus Implicancias e Implementación*. Trabajo de titulación (Licenciatura en Sistemas). Argentina: Universidad Tecnológica Nacional, 2007. 278 p.

Las 75 Herramientas de Seguridad Más Usadas. Editor ThiOsk. Disponible en: http://insecure.org/. Fecha de consulta 20 de Febrero del 2012.

BORGHELLO, C. *Op. cit.*

HERZOG, P. *Op. cit.*

BELLO, C. *Manual de seguridad en redes* [en línea]. Argentina: Editor ArCert. 2011. Disponible en: http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf.

HERZOG, P. *Op. cit.*

HERZOG, P. *Op. cit.*

Gestión de Incidentes – Análisis Forense. Editor IBM Corporation. Disponible en: http://www.asiap.org/AsIAP/images/stories/JIAP/jiap2011/Presentaciones/Azul/A1715_IBM.pdf. Fecha de consulta 15 de Febrero del 2012.

LOPEZ, M. *Análisis Forense Digital* [en línea]. 2a ed. México: Hackers & Seguridad. 2007. Disponible en: http://oas.org/juridico/spanish/cyb_analisis_foren.pdf.

LOPEZ, M. *Ibídem.*

LOPEZ, M. *Ibídem.*

BORGHELLO, C. *Op. cit.*

LOPEZ, M. *Op. cit.*

VALDESPINO, A. *Propuesta de una metodología de análisis forense para PDA (Asistentes Personales Digitales).* Trabajo de titulación (Maestro en Ciencias de Ingeniería en Microelectrónica). México: Instituto Politécnico Nacional, 2009. 58p.

BORGHELLO, C. *Op. cit.*

BORGHELLO, C. *Op. cit.*

HERZOG, P. *Op .cit.*

HERZOG, P. *Op. cit.*

HERZOG, P. *Op. cit.*

HERZOG, P. *Op. cit.*

HERZOG, P. *Op. cit.*

HERZOG, P. *Op. cit.*

HERZOG, P. *Op. cit.*

HERZOG, P. *Op. cit.*

ANEXOS

ANEXO Nº 1

VARIABLES DE LA IDEA A DEFENDER

Identificación de variables.

Se identificó como elementos de la idea a defender:

Unidad de observación:	Servidores
Variable independiente:	Metodología
Variable dependiente 1:	Testeo de seguridad
Variable dependiente 2:	Recuperación de evidencia
Enlace lógico:	Permitirá.

Definición de variables.

La definición de variables se lo realizo de manera conceptual y operacional, obteniendo los siguientes resultados:

- Definición Conceptual.

Idea a defender	Variables	Definición conceptual
La aplicación de una metodología desarrollada para la identificación de vulnerabilidades y análisis forense, permitirá un eficiente testeo de seguridad y recuperación de evidencia de los servidores de una organización.	Metodología	Métodos de investigación que se siguen para alcanzar los objetivos en una ciencia o estudio.
	Testeo de seguridad	Examinar que tan invulnerable o exento se esta de todo daño o riesgo con el fin de proteger.
	Recuperación de evidencia	Volver a poner en servicio lo que ya estaba dado por perdido con el fin de rescatar y dar seguridad.

- Definición Operacional.

Variables	Definición conceptual	Dimen-siones	Indicadores	Ítems	Apli-Cado
Metodología	Métodos de investigación que se siguen para alcanzar los objetivos en una ciencia o estudio.	Métodos	Estándares y normas	1,2,3	Administrador
			Procedimientos preventivos	4,5	
			Herramientas	6,7	
		Ciencia	Tecnología	8,9	
			Conocimiento	10,11	
Testeo de seguridad	Examinar que tan invulnerable o exento se esta de todo daño o riesgo con el fin de proteger los servidores.	Examinar	Vulnerabilidades	1	Administrador , Directores y Personal Administrativo
			Accesos	2	
			Amenazas	3,4	
		Riesgo	Identificar vulnerabilidad	5	
			Frecuencia	6	
		Proteger	Corregir vulnerabilidad	7	
			Documentar vulnerabilidad	8	
Recuperación de evidencia	Volver a poner en servicio lo que ya estaba dado por perdido con el fin de rescatar y dar seguridad a los servidores.	Servicio	Análisis forense	9	Administrador, Directores y Personal Administrativo
			Identificar evidencias	10	
		Rescatar	Encontrar evidencias	11	
			Preservar las evidencias	12	
			Analizar las evidencias	13	
		Servidores	Documentar evidencias	14	
			Presentar resultados	15	

ANEXO Nº 2

LISTA DE MÓDULOS DEL MAPA DE SEGURIDAD DE LA METODOLOGÌA OSSTMM

Sección 1 -Seguridad de la Información

1. Revisión de la Inteligencia Competitiva
2. Revisión de Privacidad
3. Recolección de Documentos

Sección 2 - Seguridad de los Procesos

1. Testeo de Solicitud
2. Testeo de Sugerencia Dirigida
3. Testeo de las Personas Confiables

Sección 3 - Seguridad en las tecnologías de Internet

1. Logística y Controles
2. Exploración de Red
3. Identificación de los Servicios del Sistema
4. Búsqueda de Información Competitiva
5. Revisión de Privacidad
6. Obtención de Documentos
7. Búsqueda y Verificación de Vulnerabilidades
8. Testeo de Aplicaciones de Internet
9. Enrutamiento
10. Testeo de Sistemas Confiados
11. Testeo de Control de Acceso
12. Testeo de Sistema de Detección de Intrusos
13. Testeo de Medidas de Contingencia
14. Descifrado de Contraseñas
15. Testeo de Denegación de Servicios
16. Evaluación de Políticas de Seguridad

Sección 4 - Seguridad en las Comunicaciones

1. Testeo de PBX
2. Testeo del Correo de Voz
3. Revisión del FAX
4. Testeo del Modem

Sección 5 - Seguridad Inalámbrica

1. Verificación de Radiación Electromagnética (EMR)
2. Verificación de Redes Inalámbricas [802.11]
3. Verificación de Redes Bluetooth
4. Verificación de Dispositivos de Entrada Inalámbricos
5. Verificación de Dispositivos de Mano Inalámbricos
6. Verificación de Comunicaciones sin Cable
7. Verificación de Dispositivos de Vigilancia Inalámbricos
8. Verificación de Dispositivos de Transacción Inalámbricos
9. Verificación de RFID
10. Verificación de Sistemas Infrarrojos
11. Revisión de Privacidad

Sección 6 - Seguridad Física

1. Revisión de Perímetro

2. Revisión de Monitoreo
3. Evaluación de Controles de Acceso
4. Revisión de Respuesta de Alarmas
5. Revisión de Ubicación
6. Revisión de Entorno

Requisitos de las Plantillas de Informes

Plantilla de Perfil de Red
Plantilla de Datos del Servidor
Plantilla de Análisis del Cortafuegos
Plantilla de Testeo Avanzado del Cortafuegos
Plantilla de Testeo de Sistemas de Detección de Intrusiones (IDS)
Plantilla de Ingeniería Social sobre el Objetivo
Plantilla de Ataque Telefónico usando Técnicas de Ingeniería Social
Plantilla de Ataque por Correo Electrónico usando Técnicas de Ingeniería Social
Plantilla de Análisis de Confianza
Plantilla de Revisión de Políticas de Privacidad
Plantilla de Revisión de Medidas de Contención
Plantilla de Correo Electrónico falseado
Plantilla de Información Competitiva
Plantilla de Ataques a Contraseñas
Plantilla de Denegación de Servicio (Denial of Service)
Plantilla de Análisis de Documentos
Plantilla de Ingeniería Social
Lista de Comprobación de Tests de Seguridad Legales
Lista de Comprobación de Tests de Seguridad Legales

ANEXO Nº 3

FASES METODOLOGÍA FORENSE SEGÚN IOCE

Fase 1 - Recolección de la Evidencia

- Garantía de calidad (enunciados generales de roles, requisitos y pruebas de aptitud del personal, documentación, herramientas y validación de las mismas y espacio de trabajo).
- Determinación de los requisitos de examen del caso.
- Principios generales que se aplican a la recuperación de la evidencia digital (recomendaciones generales, documentación y responsabilidad).

Fase 2 - Autenticación de la Evidencia

- Prácticas aplicables al examen de la evidencia de digital.
- Localización y recuperación de la evidencia de digital en la escena: precauciones, búsqueda en la escena, recolección de la evidencia y empaquetado, etiquetando y documentación.
- Priorización de la evidencia.

Fase 3 - Análisis

- Examinar la evidencia: protocolos de análisis y expedientes de caso.
- Evaluación e interpretación de la evidencia

Fase 4 - Reporte Final

- Presentación de resultados (informe escrito).
- Revisión del archivo del caso: Revisión técnica y revisión administrativa.
- Presentación oral de la evidencia.
- Procedimientos de seguridad y quejas.

ANEXO Nº 4

FASES DEL SGSI DETERMINADO POR NB ISO/IEC 27001

Fase Plan (Planificar): establecer el SGSI, sirve para planificar la organización básica, establecer los objetivos de seguridad de la información y escoger los controles adecuados de seguridad.

- Determinación del alcance del SGSI;
- Redacción de una Política de SGSI;
- Identificación de la metodología para evaluar los riesgos y determinar los criterios para la aceptabilidad de riesgos;
- Identificación de activos, vulnerabilidades y amenazas;
- Evaluación de la magnitud de los riesgos;
- Identificación y evaluación de opciones para el tratamiento de riesgos;
- Selección de controles para el tratamiento de riesgos;
- Obtención de la aprobación de la gerencia para los riesgos residuales;
- Obtención de la aprobación de la gerencia para la implementación del SGSI;
- Redacción de una declaración de aplicabilidad que detalle todos los controles aplicables, determine cuáles ya han sido implementados y cuáles no son aplicables.

Fase Do (Hacer): implementar y utilizar el SGSI, implica la realización de todo lo planificado en la anterior fase.

- Redacción de un plan de tratamiento del riesgo que describe quién, cómo, cuándo y con qué presupuesto se deberían implementar los controles correspondientes;
- Implementación de un plan de tratamiento del riesgo;
- Implementación de los controles de seguridad correspondientes;
- Determinación de cómo medir la eficacia de los controles;
- Realización de programas de concienciación y capacitación de empleados;
- Gestión del funcionamiento normal del SGSI;
- Gestión de los recursos del SGSI;
- Implementación de procedimientos para detectar y gestionar incidentes de seguridad.

FaseCheck (Verificar): monitorizar y revisar el SGSI, con el objetivo de monitorear el funcionamiento del SGSI mediante diversos canales y verificar si los resultados cumplen los objetivos establecidos.

- Implementación de procedimientos y demás controles de supervisión y control para determinar cualquier violación, procesamiento incorrecto de datos, si las actividades de seguridad se desarrollan de acuerdo a lo previsto, etc.;
- Revisiones periódicas de la eficacia del SGSI;
- Medición la eficacia de los controles;
- Revisión periódica de la evaluación de riesgos;
- Auditorías internas planificadas;
- Revisiones por parte de la dirección para asegurar el funcionamiento del SGSI y para identificar oportunidades de mejoras;
- Actualización de los planes de seguridad para tener en cuenta otras actividades de supervisión y revisión;
- Mantenimiento de registros de actividades e incidentes que puedan afectar la eficacia del SGSI.

Fase Act (Actuar): mantener y mejorar el SGSI, con el objetivo de mejor todos los incumplimientos detectados en la fase anterior.

- Implementación en el SGSI de las mejoras identificadas;
- Toma de medidas correctivas y preventivas y aplicación de experiencias de seguridad propias y de terceros;
- Comunicación de actividades y mejoras a todos los grupos de interés;
- Asegurar que las mejoras cumplan los objetivos previstos.

ANEXO Nº 5

DOMINIOS (11), OBJETIVOS DE CONTROL (39) Y CONTROLES (133) DE NB ISO/IEC 27002

5. POLÍTICA DE SEGURIDAD.

5.1 Política de seguridad de la información.
- 5.1.1 Documento de política de seguridad de la información.
- 5.1.2 Revisión de la política de seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.

6.1 Organización interna.
- 6.1.1 Compromiso de la Dirección con la seguridad de la información.
- 6.1.2 Coordinación de la seguridad de la información.
- 6.1.3 Asignación de responsabilidades relativas a la seg. de la informac.
- 6.1.4 Proceso de autorización de recursos para el tratamiento de la información.
- 6.1.5 Acuerdos de confidencialidad.
- 6.1.6 Contacto con las autoridades.
- 6.1.7 Contacto con grupos de especial interès.
- 6.1.8 Revisión independiente de la seguridad de la información.

6.2 Terceros.
- 6.2.1 Identificación de los riesgos derivados del acceso de terceros.
- 6.2.2 Tratamiento de la seguridad en la relación con los clientes.
- 6.2.3 Tratamiento de la seguridad en contratos con terceros.

7. GESTIÓN DE ACTIVOS.

7.1 Responsabilidad sobre los activos.
- 7.1.1 Inventario de activos.
- 7.1.2 Propiedad de los activos.
- 7.1.3 Uso aceptable de los activos.

7.2 Clasificación de la información.
- 7.2.1 Directrices de clasificación.
- 7.2.2 Etiquetado y manipulado de la información.

8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

8.1 Antes del empleo.
- 8.1.1 Funciones y responsabilidades.
- 8.1.2 Investigación de antecedentes.
- 8.1.3 Términos y condiciones de contratación.

8.2 Durante el empleo.
- 8.2.1 Responsabilidades de la Dirección.
- 8.2.2 Concienciación, formación y capacitación en seg. de la informac.
- 8.2.3 Proceso disciplinario.

8.3 Cese del empleo o cambio de puesto de trabajo.
- 8.3.1 Responsabilidad del cese o cambio.
- 8.3.2 Devolución de activos.
- 8.3.3 Retirada de los derechos de acceso.

9. SEGURIDAD FÍSICA Y DEL ENTORNO.

9.1 Áreas seguras.
- 9.1.1 Perímetro de seguridad física.
- 9.1.2 Controles físicos de entrada.
- 9.1.3 Seguridad de oficinas, despachos e instalaciones.
- 9.1.4 Protección contra las amenazas externas y de origen ambiental.
- 9.1.5 Trabajo en áreas seguras.
- 9.1.6 Áreas de acceso público y de carga y descarga.

9.2 Seguridad de los equipos.
- 9.2.1 Emplazamiento y protección de equipos.
- 9.2.2 Instalaciones de suministro.
- 9.2.3 Seguridad del cableado.
- 9.2.4 Mantenimiento de los equipos.
- 9.2.5 Seguridad de los equipos fuera de las instalaciones.
- 9.2.6 Reutilización o retirada segura de equipos.
- 9.2.7 Retirada de materiales propiedad de la empresa.

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.

10.1 Responsabilidades y procedimientos de operación.
- 10.1.1 Documentación de los procedimientos de operación.
- 10.1.2 Gestión de cambios.
- 10.1.3 Segregación de tareas.
- 10.1.4 Separación de los recursos de desarrollo, prueba y operación.

10.2 Gestión de la provisión de servicios por terceros.
- 10.2.1 Provisión de servicios.
- 10.2.2 Supervisión y revisión de los servicios prestados por terceros.
- 10.2.3 Gestión del cambio en los servicios prestados por terceros.

10.3 Planificación y aceptación del sistema.
- 10.3.1 Gestión de capacidades.
- 10.3.2 Aceptación del sistema.

10.4 Protección contra el código malicioso y descargable.
- 10.4.1 Controles contra el código malicioso.
- 10.4.2 Controles contra el código descargado en el cliente.

10.5 Copias de seguridad.
- 10.5.1 Copias de seguridad de la información.

10.6 Gestión de la seguridad de las redes.
- 10.6.1 Controles de red.
- 10.6.2 Seguridad de los servicios de red.

10.7 Manipulación de los soportes.
- 10.7.1 Gestión de soportes extraíbles.
- 10.7.2 Retirada de soportes.
- 10.7.3 Procedimientos de manipulación de la información.
- 10.7.4 Seguridad de la documentación del sistema.

10.8 Intercambio de información.
- 10.8.1 Políticas y procedimientos de intercambio de información.
- 10.8.2 Acuerdos de intercambio.
- 10.8.3 Soportes físicos en tránsito.
- 10.8.4 Mensajería electrónica.
- 10.8.5 Sistemas de información empresariales.

10.9 Servicios de comercio electrónico.
- 10.9.1 Comercio electrónico.
- 10.9.2 Transacciones en línea.
- 10.9.3 Información públicamente disponible.

10.10 Supervisión.
- 10.10.1 Registros de auditoría.
- 10.10.2 Supervisión del uso del sistema.
- 10.10.3 Protección de la información de los registros.
- 10.10.4 Registros de administración y operación.
- 10.10.5 Registro de fallos.
- 10.10.6 Sincronización del reloj.

11. CONTROL DE ACCESO.

11.1 Requisitos de negocio para el control de acceso.
- 11.1.1 Política de control de acceso.

11.2 Gestión de acceso de usuario.
- 11.2.1 Registro de usuario.
- 11.2.2 Gestión de privilegios.
- 11.2.3 Gestión de contraseñas de usuario.
- 11.2.4 Revisión de los derechos de acceso de usuario.

11.3 Responsabilidades de usuario.
- 11.3.1 Uso de contraseñas.
- 11.3.2 Equipo de usuario desatendido.
- 11.3.3 Política de puesto de trabajo despejado y pantalla limpia.

11.4 Control de acceso a la red.
- 11.4.1 Política de uso de los servicios en red.
- 11.4.2 Autenticación de usuario para conexiones externas.
- 11.4.3 Identificación de los equipos en las redes.
- 11.4.4 Protección de los puertos de diagnóstico y configuración remotos.
- 11.4.5 Segregación de las redes.
- 11.4.6 Control de la conexión a la red.
- 11.4.7 Control de encaminamiento (routing) de red.

11.5 Control de acceso al sistema operativo.
- 11.5.1 Procedimientos seguros de inicio de sesión.
- 11.5.2 Identificación y autenticación de usuario.
- 11.5.3 Sistema de gestión de contraseñas.
- 11.5.4 Uso de los recursos del sistema.
- 11.5.5 Desconexión automática de sesión.
- 11.5.6 Limitación del tiempo de conexión.

11.6 Control de acceso a las aplicaciones y a la información.
- 11.6.1 Restricción del acceso a la información.
- 11.6.2 Aislamiento de sistemas sensibles.

11.7 Ordenadores portátiles y teletrabajo.
- 11.7.1 Ordenadores portátiles y comunicaciones móviles.
- 11.7.2 Teletrabajo.

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.

12.1 Requisitos de seguridad de los sistemas de información.
- 12.1.1 Análisis y especificación de los requisitos de seguridad.

12.2 Tratamiento correcto de las aplicaciones.
- 12.2.1 Validación de los datos de entrada.
- 12.2.2 Control del procesamiento interno.
- 12.2.3 Integridad de los mensajes.
- 12.2.4 Validación de los datos de salida.

12.3 Controles criptográficos.
- 12.3.1 Política de uso de los controles criptográficos.
- 12.3.2 Gestión de claves.

12.4 Seguridad de los archivos de sistema.
- 12.4.1 Control del software en explotación.
- 12.4.2 Protección de los datos de prueba del sistema.
- 12.4.3 Control de acceso al código fuente de los programas.

12.5 Seguridad en los procesos de desarrollo y soporte.
- 12.5.1 Procedimientos de control de cambios.
- 12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
- 12.5.3 Restricciones a los cambios en los paquetes de software.
- 12.5.4 Fugas de información.
- 12.5.5 Externalización del desarrollo de software.

12.6 Gestión de la vulnerabilidad técnica.
- 12.6.1 Control de las vulnerabilidades técnicas.

13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

13.1 Notificación de eventos y puntos débiles de seguridad de la información.
- 13.1.1 Notificación de los eventos de seguridad de la información.
- 13.1.2 Notificación de puntos débiles de seguridad.

13.2 Gestión de incidentes y mejoras de seguridad de la información.
- 13.2.1 Responsabilidades y procedimientos.
- 13.2.2 Aprendizaje de los incidentes de seguridad de la información.
- 13.2.3 Recopilación de evidencias.

14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
- 14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
- 14.1.2 Continuidad del negocio y evaluación de riesgos.
- 14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.
- 14.1.4 Marco de referencia para la planificación de la cont. del negocio.
- 14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.

15. CUMPLIMIENTO.

15.1 Cumplimiento de los requisitos legales.
- 15.1.1 Identificación de la legislación aplicable.
- 15.1.2 Derechos de propiedad intelectual (DPI).
- 15.1.3 Protección de los documentos de la organización.
- 15.1.4 Protección de datos y privacidad de la información de carácter personal.
- 15.1.5 Prevención del uso indebido de recursos de tratamiento de la información.
- 15.1.6 Regulación de los controles criptográficos.

15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.
- 15.2.1 Cumplimiento de las políticas y normas de seguridad.
- 15.2.2 Comprobación del cumplimiento técnico.

15.3 Consideraciones sobre las auditorías de los sistem. de información.
- 15.3.1 Controles de auditoría de los sistemas de información.
- 15.3.2 Protección de las herramientas de auditoría de los sist. de inform.

www.iso27002.cl

ANEXO Nº 6

DETERMINACIÓN DEL TAMAÑO DE LA MUESTRA

Con el propósito de recolectar información referente a la seguridad de los servidores de la institución, basado en los objetivos y el alcance de la investigación, se determino como universo poblacional de la E.S.F.M. E.A. un total de 1640 personas, de los cuales:

- 1500 alumnos inscritos en diferentes especialidades; 797 son del sistema semestral y 703 del sistema anual.
- 104 profesores docentes.
- 3 directores; general, académico, administrativo y financiero
- 27 funcionarios administrativos
- 6 funcionarios de servicio

Uso de los servidores por el universo poblacional "E.S.F.M. E.A"

Personas	N° Personas	Uso Servidor-1	Uso Servidor-2	Uso Servidor-3
Alumnos	1500	5%	--	--
Docentes	104	5%	--	--
Directores	3	10%	30%	1%
Administrativos	27	50%	100%	30%
Servicio	6	--	--	--
Totales	1640			

Fuente: Elaboración propia en base a información proporcionada por el administrador de los servidores.

Al no existir un tamaño ideal de muestra poblacional porque su elección depende de las características del objeto de estudio y este debe ser proporcional y representativo al universo poblacional; se determino aplicar la metodología propuesta al servidor-2 por su utilidad e información administrada. Razón por la que se seleccionó mediante el método no probabilístico "Muestreo de Selección Experta" la muestra poblacional de 30 personas; conformada por directores y administrativos (incluye el administrador del servidor), quienes están siendo afectados por el problema al tener acceso continuo a los diferentes servicios de este servidor para consulta o modificación de datos.

ANEXO Nº 7

ENCUESTA

(Dirigido al Administrador del Servidor, Directores y Personal Administrativo)

Buenos días (tardes):

Me dirijo a su persona con el objeto de elaborar una tesis para la identificación de vulnerabilidades y análisis forense en los servidores de la institución "ESFM EA". Por lo cual pido su ayuda para que conteste algunas preguntas. Sus respuestas serán confidenciales y anónimas.

INSTRUCTIVO. Lea atentamente cada una de las preguntas antes de responder, y marque con una "X" en la casilla correspondiente.

Ítem 1: ¿Sabe que es una vulnerabilidad con relación a equipos servidores de una institución?

Si	
No	

Ítem 2: ¿Se realiza el control de acceso de usuarios a los servidores, mediante la asignación de usuarios y contraseñas?

Si	
No	

Ítem 3: ¿Cuáles son las amenazas más frecuentes que tienen los servidores?

Virus	
Mala configuración de sistemas	
Acceso no autorizado mediante la red internet	
Sucesos de origen físico (goteras, polvo, sobre carga eléctrica, etc.)	

Ítem 4: ¿Qué respuestas o medidas se asumen ante amenazas por ataques a los servidores?

Desconectar el servidor temporalmente de la red	
Escanear el servidor para detectar virus	
Realizar test de seguridad para detectar fallas	
Examinar físicamente el servidor, dispositivos conectados y/o verificar sistemas afectados	

Ítem 5: ¿Cuánto tiempo se tarda en identificar una vulnerabilidad en los equipos servidores?

No se detectan vulnerabilidades	
0 a 4 hora(s)	
4 a 8 hora(s)	
1 día	
Varios días	

Ítem 6: ¿Por la existencia de vulnerabilidades con que frecuencia se tienen ataques en los servidores por parte de usuarios o personas ajenas a la institución?

No se tienen ataques	
Cada día	
A la Semana	
Al Mes	

Ítem 7: ¿Cómo se corrigen las vulnerabilidades encontradas en los equipos servidores?

No se corrigen, se instala todo nuevamente	
Se aplican parches de seguridad (actualización de vacunadores, sistema operativo, etc.)	
Se protegen puertos abiertos, restringen accesos de usuarios, cambio de contraseñas, otros.	

Ítem 8: ¿Cómo se documentan las vulnerabilidades encontradas en los equipos servidores?

No se documentan	
Se elabora un breve informe y se registran en plantillas o formularios de elaboración propia	
Se elabora un informe completo con formularios de registro internacional	

Ítem 9: ¿Sabe que es realizar análisis forense a equipos servidores de una institución?

Si	
No	

Ítem 10: ¿Ante actos de criminalidad (fraude, robo, espionaje, virus, etc.) en los equipos servidores, se realiza identificación de evidencias?

Si	
No	

Ítem 11: ¿Ante actos de criminalidad (fraude, robo, espionaje, virus, etc.) en los equipos servidores, se encuentran evidencias físicas o lógicas?

Si	
No	

Ítem 12: ¿De las evidencias encontradas en los equipos servidores, se preservan evidencias de intrusión?

Si	
No	

Ítem 13: ¿Se realiza análisis de evidencia a las intrusiones detectadas en los servidores con el fin de determinar quiénes fueron, cómo ingresaron, su objetivo y/o qué daño causaron?

Si	
No	

Ítem 14: ¿Cómo se documentan las evidencias de ataque a los equipos servidores?

No se documentan	
Se elabora un breve informe y se registran en plantillas o formularios de elaboración propia	
Se elabora un informe completo con formularios de registro internacional	

Ítem 15: ¿Cómo se presentan y socializan las evidencias de criminalidad encontradas en los servidores de la institución?

No se presentan	
Formalmente	
Informalmente	

GRACIAS POR SU VALIOSA COLABORACIÓN.

ANEXO Nº 8

GUÍA DE ENTREVISTA
(Dirigido al Administrador del Servidor)

Buenos días (tardes):

Me dirijo a su persona con el objeto de elaborar una tesis para identificar vulnerabilidades y realizar análisis forense en servidores. Por lo cual pido su ayuda para que conteste algunas preguntas con respecto a los servidores de la institución "ESFM EA":

Ítem 1: ¿Qué estándares y/o normas científicas de seguridad de la información utiliza para identificar vulnerabilidades en servidores?, mencionar y describir.

Ítem 2: ¿Qué estándares y/o normas científicas de seguridad de la información utiliza para hacer análisis forense en servidores?, mencionar y describir.

Ítem 3: ¿Con el fin de direccionar y gestionar de manera rápida y eficaz los problemas de seguridad en los servidores, aprueba la aplicación de una metodología estandarizada basado en normas para identificar vulnerabilidades y hacer análisis forense, porque?

Ítem 4: ¿Mediante qué procedimientos preventivos da seguridad a servidores?

Ítem 5: ¿Qué procedimientos de investigación conoce usted para identificar vulnerabilidades y realizar análisis forense en servidores?

Ítem 6: ¿Qué herramientas utiliza para detectar las vulnerabilidades de los servidores?, mencionar y describir.

Ítem 7: ¿Qué herramientas utiliza para recuperar evidencia de los servidores?, mencionar y describir.

Ítem 8: ¿En cuanto a tecnología de hardware qué dispositivos de seguridad tienen los servidores?, mencionar características principales en cada caso.

Ítem 9: ¿En cuanto a tecnología de software qué plataforma de sistema operativo, configuración y aplicaciones instaladas tienen los servidores?, mencionar y describir.

Ítem 10: ¿Cuál es el nivel de conocimiento que tiene usted en identificar vulnerabilidades de servidores?

Ítem 11: ¿Cuál es el nivel de conocimiento que tiene usted para realizar análisis forense a servidores?

ANEXO Nº 9

GUÍA DE OBSERVACIÓN

(Dirigido al Administrador del Servidor, Directores y Personal Administrativo)

ACTIVIDADES.

1) Se registra:

Las actividades realizadas por el administrador del servidor:

- Configuración de direcciones IP asignados a cada servidor y equipos clientes.
- Configuración de sistemas y utilitarios en los servidores.
- Accesos y contraseñas de usuarios.

Las actividades realizadas por personal directivo: No llevan ningún registro.

Las actividades realizadas por personal administrativo:

- Configuración de dirección IP de los servidores y equipo asignado.
- Manejo de dispositivos físicos (impresoras, portátiles, etc.).
- Usuarios y contraseñas.

2) Servicios utilizados del servidor-2:

Administrador del servidor y personal administrativo:

- Servicio de internet
- Acceso a los sistemas de inscripciones y calificaciones, otros sistemas
- Acceso a compartir dispositivos físicos
- Acceso a compartir archivos

Directores:

- Servicio de internet
- Acceso a compartir archivos

- Obtiene solo información impresa

3) Actos de criminalidad:

Administrador del servidor: No realiza actos de criminalidad

Directores y personal administrativo:

- Accesos no autorizados por curiosidad, sabotaje, robo de información, entre otros.
- Contagio de virus de manera no intencionada

4) Problemas ocasionados:

Administrador del servidor; por falta de aplicación y/o conocimiento de métodos de seguridad:

- Mal funcionamiento o inhabilitación del servidor
- Acceso libre a información confidencial de los sistemas institucionales
- Problemas con programas maliciosos (virus, troyanos, gusanos, etc.)

Directores y personal administrativo; por actos de criminalidad:

- Bajo rendimiento en la velocidad de trasmisión de datos del servidor y la red
- No se tiene servicio de internet
- No se puede acceder a los sistemas de la institución
- Contagio de virus, en los servidores y clientes
- Robo de información confidencial

ANEXO Nº 10

ANÁLISIS E INTERPRETACIÓN A LOS RESULTADOS DE LA ENCUESTA

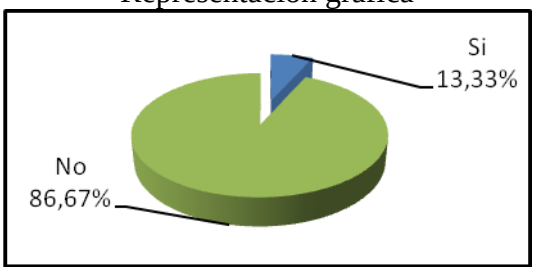
Ítem 1: ¿Sabe que es una vulnerabilidad con relación a equipos servidores de una institución?

Cuadro estadístico

Alternativa	Frecuencia	Porcentaje
Si	4	13,33
No	26	86,67
Totales	**30**	**100**

Fuente: Elaboración propia en base a resultados tabulados del ítem 1 de la encuesta.

Representacion gráfica



Fuente: Elaboración propia en base a cuadro estadístico ítem 1.

Del total de la muestra el 86,67% no tenía conocimiento de lo que significaba la existencia de vulnerabilidades en los servidores de la institución, limitándose a recibir información haciendo uso de algunos servicios y exigir un buen funcionamiento. Solo el 13,33% tenía conocimiento, por consiguiente comprendía la importancia de corregir las vulnerabilidades para proteger la información, evitar riesgos por fraude, robo, goteras, sobrecarga eléctrica, entre otros.

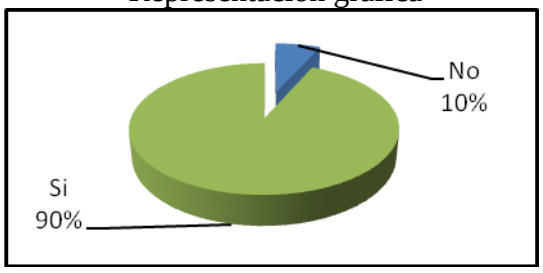
Ítem 2: ¿Se realiza el control de acceso de usuarios a los servidores, mediante la asignación de usuarios y contraseñas?

Cuadro estadístico

Alternativa	Frecuencia	Porcentaje
Si	27	90
No	3	10
Totales	**30**	**100**

Fuente: Elaboración propia en base a resultados tabulados del ítem 2 de la encuesta.

Representacion gráfica



Fuente: Elaboración propia en base a cuadro estadístico ítem 2.

El 90% de la población muestral confirmó que si existe control de acceso a los servidores mediante usuarios y contraseñas; mientras que el 10% manifestó que no, significando que probablemente acceden libremente a información y servicios de los servidores, convirtiéndose en intrusos que podrían provocar daños o fallas a los servidores.

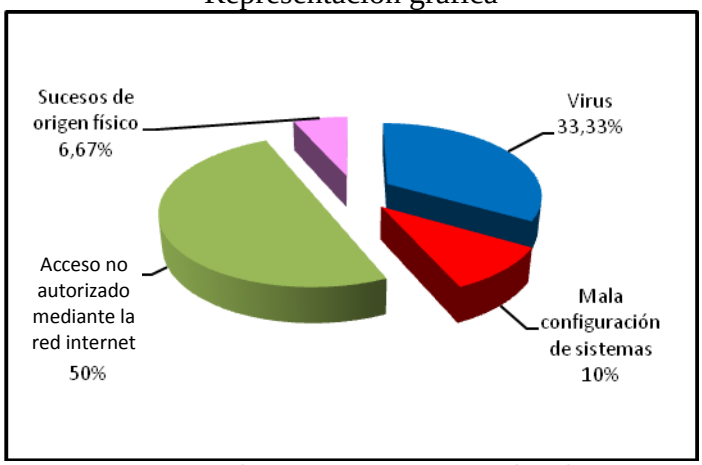
Ítem 3: ¿Cuáles son las amenazas más frecuentes que tienen los servidores?

Cuadro estadístico

Alternativa	Frecuencia	Porcentaje
Virus	10	33,33
Mala configuración de sistemas	3	10
Acceso no autorizado mediante la red internet	15	50
Sucesos de origen físico (goteras, polvo, sobre carga eléctrica, etc.)	2	6,67
Totales	**30**	**100**

Fuente: Elaboración propia en base a resultados tabulados del ítem 3 de la encuesta.

Representación gráfica



Fuente: Elaboración propia en base a cuadro estadístico ítem 3.

Los resultados muestran que el servidor de la institución era amenazado en un 50% por acceso no autorizado mediante la red internet, mientras un 33,33% por virus, el 10% por mala configuración de sistemas (operativo e institucionales) y el 6,67% por sucesos de origen físico como las goteras, polvo, sobre carga eléctrica, entre otros. Afectando al buen funcionamiento del servidor, ocasionado incumplimiento de actividades laborares y objetivos institucionales.

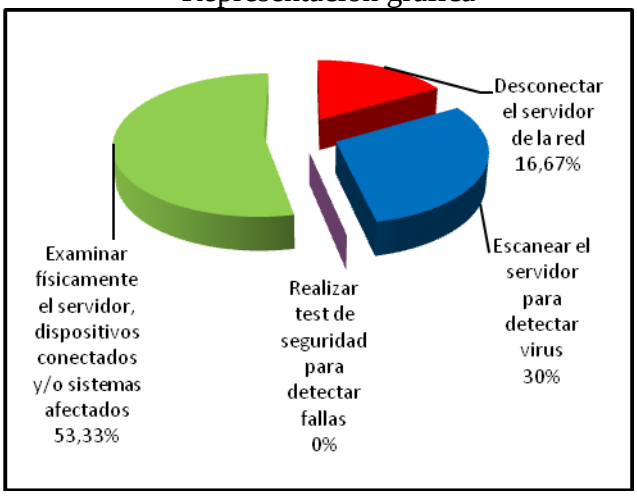
Ítem 4: ¿Qué respuestas o medidas se asumen ante amenazas por ataques a los servidores?

Cuadro estadístico

Alternativa	Frecuencia	Porcentaje
Desconectar el servidor temporalmente de la red	5	16,67
Escanear el servidor para detectar virus	9	30
Realizar test de seguridad para detectar fallas	0	0
Examinar físicamente el servidor, dispositivos conectados y/o verificar sistemas afectados	16	53,33
Totales	**30**	**100**

Fuente: Elaboración propia en base a resultados tabulados del ítem 4 de la encuesta.

Representación gráfica



Fuente: Elaboración propia en base a cuadro estadístico ítem 4.

Los resultados indican la solución que el administrador efectuaba ante amenazas que ocasionaban daños o fallas en los servidores. Un 53,33% afirmaba que se examina físicamente el servidor, dispositivos conectados (routers, módems, etc.) y/o se verifican sistemas afectados (operativo e instituciones), el 30% indicó que se escanea con vacunadores para detectar virus, mientras el 16,67% menciono que se desconecta temporalmente el servidor de la red.

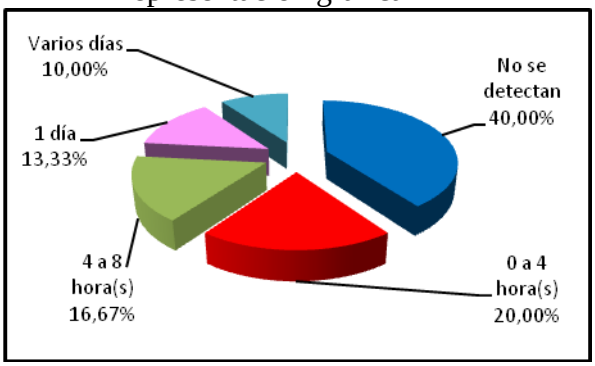
Ítem 5: ¿Cuánto tiempo se tarda en identificar una vulnerabilidad en los equipos servidores?

Cuadro estadístico

Alternativa	Frecuencia	Porcentaje
No se detectan	12	40
0 a 4 hora(s)	6	20
4 a 8 hora(s)	5	16,67
1 día	4	13,33
Varios días	3	10
Totales	**30**	**100**

Fuente: Elaboración propia en base a resultados tabulados del ítem 5 de la encuesta.

Representación gráfica



Fuente: Elaboración propia en base a cuadro estadístico ítem 5.

Debe tenerse en cuenta que cada vulnerabilidad en los servidores es diferente, requiere tiempo de respuesta agiles, sin embargo su tratamiento y tiempo de solución varía, depende de la complejidad, capacidad y conocimiento del administrador; pero un 40% de la muestra indicó que no se detectan vulnerabilidades, el 20% señaló como máximo tarda 4 horas, un 16,67% mencionó de 4 a 8 horas, el 13,33% indica que tarda un día y el 10% insinuó tarda varios días.

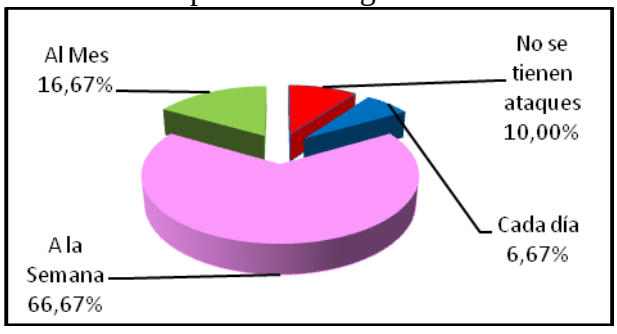
Ítem 6: ¿Por la existencia de vulnerabilidades con que frecuencia se tienen ataques en los servidores por parte de usuarios o personas ajenas a la institución?

Cuadro estadístico

Alternativa	Frecuencia	Porcentaje
No se tienen ataques	3	10
Cada día	2	6,67
A la Semana	20	66,67
Al Mes	5	16,67
Totales	**30**	**100**

Fuente: Elaboración propia en base a resultados tabulados del ítem 6 de la encuesta.

Representación gráfica



Fuente: Elaboración propia en base a cuadro estadístico ítem 6.

Un 66,67% de la población encuestada tenia conocimiento de la existencia de intrusos internos o externos que aprovechando las vulnerabilidades de los servidores accedían sin autorización en promedio a la semana una vez, mientras el 16,67% indica que esto ocurre al mes, un 10% indico que no se tiene ningún tipo de ataque y el 6,67% menciona que esto sucede cada día.

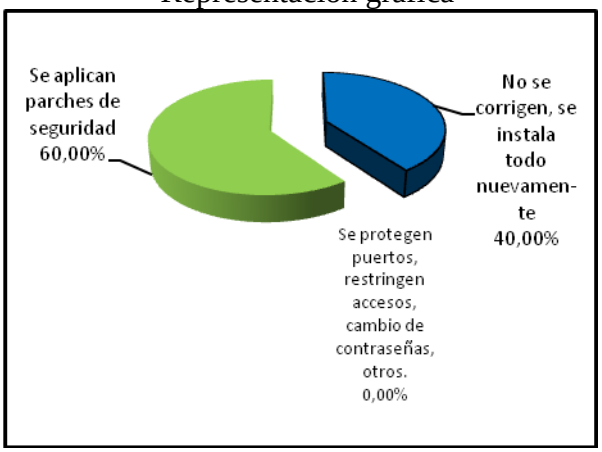
Ítem 7: ¿Cómo se corrigen las vulnerabilidades encontradas en los equipos servidores?

Cuadro estadístico

Alternativa	Frecuencia	Porcentaje
No se corrigen, se instala todo nuevamente	12	40
Se aplican parches de seguridad (actualización de vacunadores, sistema operativo, etc.)	18	60
Se protegen puertos abiertos, restringen accesos de usuarios, cambio de contraseñas, otros.	0	0
Totales	**30**	**100**

Fuente: Elaboración propia en base a resultados tabulados del ítem 7 de la encuesta.

Representación gráfica



Fuente: Elaboración propia en base a cuadro estadístico ítem 7.

Es de mucha importancia dar seguridad a los servidores de la institución priorizando y remediando con efectividad las vulnerabilidades, sin embargo el 60% de los encuestados menciono que solo se aplican parches de seguridad actualizando vacunadores, sistemas, otros. Pero un 40% manifiesto que no se corrigen las vulnerabilidades se instala todo nuevamente.

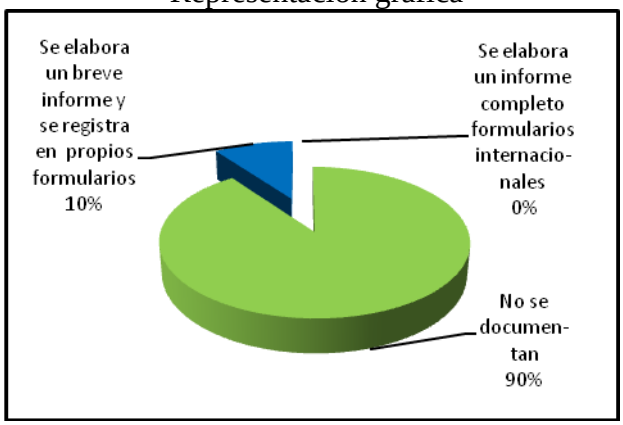
Ítem 8: ¿Cómo se documentan las vulnerabilidades encontradas en los equipos servidores?

Cuadro estadístico

Alternativa	Frecuencia	Porcentaje
No se documentan	27	90
Se elabora un breve informe y se registran en plantillas o formularios de elaboración propia	3	10
Se elabora un informe completo con formularios de registro internacional	0	0
Totales	**30**	**100**

Fuente: Elaboración propia en base a resultados tabulados del ítem 8 de la encuesta.

Representación gráfica



Fuente: Elaboración propia en base a cuadro estadístico ítem 8.

Un grupo mayor de la muestra poblacional 90% menciono que no se documentan las vulnerabilidades detectadas en los servidores de la institución, solo un 10% afirma que el administrador del servidor elabora un breve informe con plantillas o formularios de vulnerabilidades. Significando que las vulnerabilidades detectadas y solucionadas de los servidores no se documentaban utilizando métodos recomendados que son claros, concisos y efectivos para gestionar las vulnerabilidades.

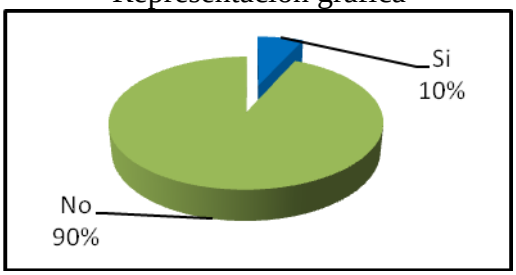
Ítem 9: ¿Sabe que es realizar análisis forense a equipos servidores de una institución?

Cuadro estadístico

Alternativa	Frecuencia	Porcentaje
Si	3	10
No	27	90
Totales	**30**	**100**

Fuente: Elaboración propia en base a resultados tabulados del ítem 9 de la encuesta.

Representación gráfica



Fuente: Elaboración propia en base a cuadro estadístico ítem 9.

De la muestra universal, el 90% no tenía conocimiento de lo que significaba realizar análisis forense, limitándose a recibir información haciendo uso de algunos servicios y exigir el buen funcionamiento de los servidores; solo un 10% de la población tenía conocimiento por lo que comprendía la importancia de analizar el servidor para buscar evidencia con el fin de utilizarlo en una negociación extrajudicial o judicialmente.

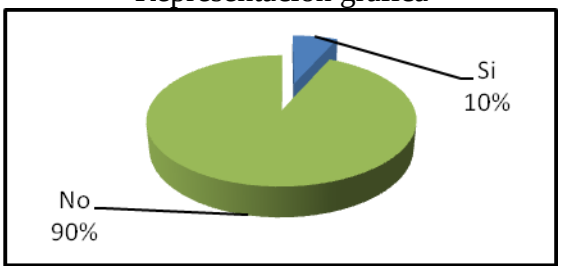
Ítem 10: ¿Ante actos de criminalidad (fraude, robo, espionaje, virus, etc.) en los equipos servidores, se realiza identificación de evidencias?

Cuadro estadístico

Alternativa	Frecuencia	Porcentaje
Si	3	10
No	27	90
Totales	**30**	**100**

Fuente: Elaboración propia en base a resultados tabulados del ítem 10 de la encuesta.

Representación gráfica



Fuente: Elaboración propia en base a cuadro estadístico ítem 10.

La evidencia es utilizada para establecer hechos relacionando diferentes eventos de criminalidad y reconociendo la frágil naturaleza de los datos digitales del servidor; sin embargo, un 90% de los encuestados menciono que no se realiza identificación de evidencias y el 10% afirma que si se realiza esta actividad.

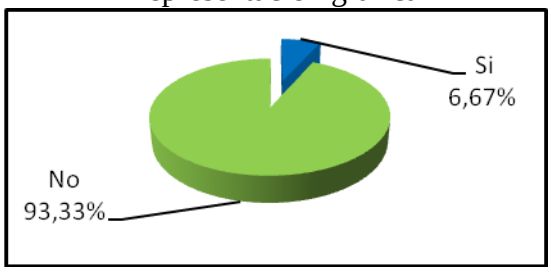
Ítem 11: ¿Ante actos de criminalidad (fraude, robo, espionaje, virus, etc.) en los equipos servidores, se encuentran evidencias físicas o lógicas?

Cuadro estadístico

Alternativa	Frecuencia	Porcentaje
Si	2	6,67
No	28	93,33
Totales	**30**	**100**

Fuente: Elaboración propia en base a resultados tabulados del ítem 11 de la encuesta.

Representación gráfica



Fuente: Elaboración propia en base a cuadro estadístico ítem 11.

Actualmente los actos de criminalidad contra los servidores, en su generalidad son de tipo lógico, se realizan mediante la red instalando o infectando un programa malicioso (virus, rootkits, spyware, entre otros), siendo mucho más complicado encontrar evidencias reales; por lo que tal vez el 93,33% de los encuestados menciono que no se encuentran evidencias. Solo un 6,67% menciono que si encuentran evidencias.

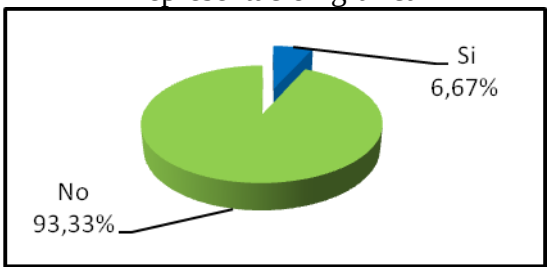
Ítem 12: ¿De las evidencias encontradas en los equipos servidores, se preservan evidencias de intrusión?

Cuadro estadístico

Alternativa	Frecuencia	Porcentaje
Si	2	6,67
No	28	93,33
Totales	**30**	**100**

Fuente: Elaboración propia en base a resultados tabulados del ítem 12 de la encuesta.

Representación gráfica



Fuente: Elaboración propia en base a cuadro estadístico ítem 12.

Para asegurar la preservación de evidencias encontradas en los servidores por actos de intrusión, requiere de un conjunto de métodos de seguridad científicamente probados contra daños accidentales o intencionales; siendo una razón por la que tal vez el 93,33% de los encuestados mencione que no se preservan evidencias, solo un grupo reducido del 6,67% confirma que si se preservan.

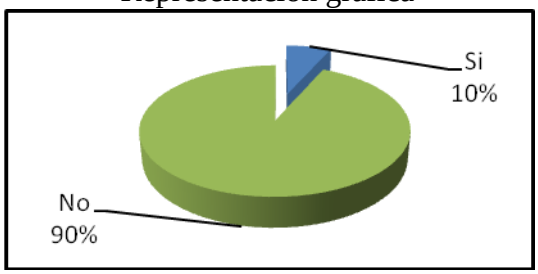
Ítem 13: ¿Se realiza análisis de evidencia a las intrusiones detectadas en los servidores con el fin de determinar quiénes fueron, cómo ingresaron, su objetivo y/o qué daño causaron?

Cuadro estadístico

Alternativa	Frecuencia	Porcentaje
Si	3	10
No	27	90
Totales	**30**	**100**

Fuente: Elaboración propia en base a resultados tabulados del ítem 13 de la encuesta.

Representación gráfica



Fuente: Elaboración propia en base a cuadro estadístico ítem 13.

El análisis de evidencia realizado a servidores, consiste en buscar información necesaria de intrusión determinando motivos, origen y causas que indujeron a cometer delito, con la finalidad de obtener evidencias. De la población encuestada el 90% menciona que no se realiza esta actividad y un grupo del 10% menciono que si.

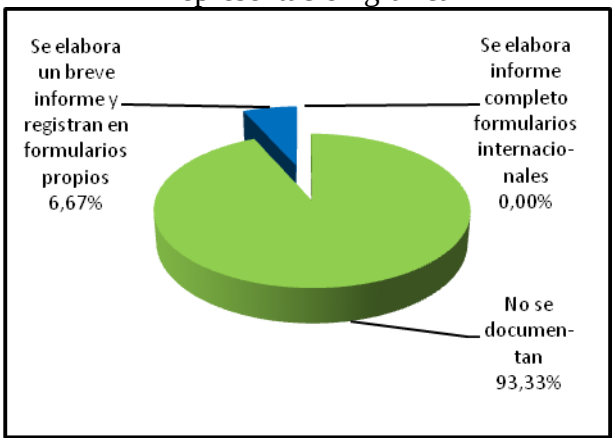
Ítem 14: ¿Cómo se documentan las evidencias de ataque a los equipos servidores?

Cuadro estadístico

Alternativa	Frecuencia	Porcentaje
No se documentan	28	93,33
Se elabora un breve informe y se registran en plantillas o formularios de elaboración propia	2	6,67
Se elabora un informe completo con formularios de registro internacional	0	0
Totales	**30**	**100**

Fuente: Elaboración propia en base a resultados tabulados del ítem 14 de la encuesta.

Representación gráfica



Fuente: Elaboración propia en base a cuadro estadístico ítem 14.

De los encuestados un alto porcentaje del 93,33% menciono que no documentan las evidencias de intrusión detectados en los servidores, solo el 6,67% indica que el administrador elabora un breve informe con plantillas y formularios propios. Significando que no se aplican métodos científicos para desarrollar informes completos de evidencias descubiertas, para que sirvan de prueba en una negociación judicial o extrajudicial.

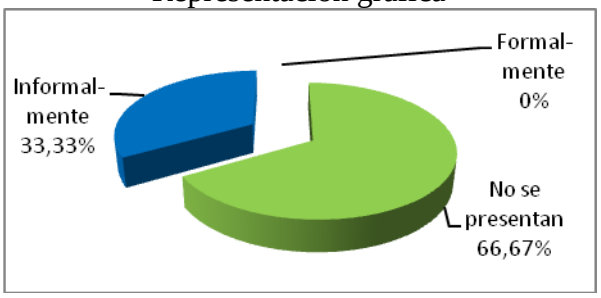
Ítem 15: ¿Cómo se presentan y socializan las evidencias de criminalidad encontradas en los servidores de la institución?

Cuadro estadístico

Alternativa	Frecuencia	Porcentaje
No se presentan	20	66,67
Informalmente	10	33,33
Formalmente	0	0
Totales	**30**	**100**

Fuente: Elaboración propia en base a resultados tabulados del ítem 15 de la encuesta.

Representación gráfica



Fuente: Elaboración propia en base a cuadro estadístico ítem 15.

Terminado una investigación de análisis forense, sus resultados se presentan a las personas indicadas para su evaluación y toma de decisiones, con la finalidad de evitar problemas similares a futuro. Sin embargo, el 66,67% de los encuestados menciono que no se realiza esta actividad y un 33,33% indicó que sucede de manera informal.

ANEXO N° 11

ENCUESTA A EXPERTOS

(Dirigido a Profesionales Especialistas)

Buenos días (tardes):

Distinguido colega, en función de obtener información acerca de la propuesta de una metodología de identificación de vulnerabilidades y análisis forense en los equipos servidores de una organización, me dirijo a usted para conocer su criterio profesional.Sus conocimientos y experiencia en problemas de seguridad informática me resultan imprescindibles, por lo que solicito su digna colaboración de manera objetiva, real y sin exceso de modestia en el análisis y valoración de las siguientes preguntas:

De antemano agradezco su valiosa colaboración y me disculpo por ocupar su preciado tiempo.

I.- Nombre:
Institución donde trabaja:
Cargo que ocupa:
Años de experiencia en su desempeño profesional:
Nivel de profesionalización y/o trabajos de investigación recientes:

II.- Marque con una X**,** en una escala creciente del 1 al 10, el valor que corresponde con el grado de conocimiento o información que tiene usted sobre el tema de estudio.

ESCALA	1	2	3	4	5	6	7	8	9	10
EXPERTO										

III.- Marque con una X**,** atendiendo las alternativas: muy adecuado (MA), bastante adecuado (BA), adecuado (A), poco adecuado (PA) e inadecuado (I), en relación a los siguientes aspectos a valorar sobre la propuesta metodológica.

No.	ASPECTOS A VALORAR	MA	BA	A	PA	I
1	¿Cómo valora el **sustento teórico** que respalda la investigación, cree que permite llegar a una conceptualización clara y comprensible sobre la identificación de vulnerabilidades y análisis forense en equipos servidores?					
2	¿Cómo considera la **sistematización de la propuesta,** cree que ofrece una orientación para identificar vulnerabilidades y realizar análisis forense a equipos servidores?					
3	¿Cómo valora el planteamiento del **objetivo general** que se alcanzó con la investigación?					
4	¿Cómo considera la importancia de incluir en la propuesta metodológica un **proceso de identificación de vulnerabilidades con sus fases de prevención, identificación y corrección**, que permite detectar y solucionar tanto las fallas como amenazas detectadas en los servidores?					
5	¿Cómo considera la importancia de incluir en la propuesta metodológica un **proceso de análisis forense con sus fases de identificación, preservación, análisis, documentación y presentación**, que permite recuperar evidencia de los servidores para dar solución a delitos informáticos?					
6	¿Cómo valora los **resultados de la aplicación de la metodología propuesta** para la identificación de vulnerabilidades y análisis forense?					

VI.- Tomando en cuenta los números correspondientes en que aparecen los diferentes aspectos de la propuesta de una metodología de identificación de vulnerabilidades y análisis forense en los servidores de una organización, diga qué modificaría, que incluiría y que eliminaría en cada uno de ellos considerando su experiencia profesional, de postgrado y/o conocimiento sobre procedimientos metodológicos en Bolivia o en el extranjero.

Nº	ASPECTOS A VALORAR	QUE MODIFICAR	QUE INCLUIR	QUE ELIMINAR
1	Sustento teórico.			
2	Sistematización de la propuesta.			
3	Objetivo general de la propuesta.			
4	Proceso de identificación de vulnerabilidades con sus fases de prevención, identificación y corrección.			
5	Proceso de análisis forense con sus fases de identificación, preservación, análisis, documentación y presentación.			
6	Resultados de la aplicación de la metodología propuesta.			

GRACIAS POR SU VALIOSA COLABORACIÓN.

ANEXO N° 12

RESUMEN DE LAS VALORACIONES DE VIABILIDAD

N° Experto	Grado de Conocimiento	Preg 1	Preg 2	Preg 3	Preg 4	Preg 5	Preg 6
1	6	4	5	4	4	4	4
2	5	5	4	4	5	5	4
3	9	3	4	4	4	4	4
4	6	5	4	5	5	5	4
5	8	3	3	3	3	3	3
6	7	5	5	4	4	4	4
7	6	4	4	4	5	5	4
PROMEDIO :		4	4,143	4	4,286	4,286	3,857
PORCENTAJE :		80	82,86	80	85,72	85,72	77,14

Según la escala:

Muy adecuado (MA)	5
Bastante adecuado (BA)	4
Adecuado (A)	3
Poco adecuado (PA)	2
Inadecuado (I)	1