FACULTAD DE INFORMATICA

UNIVERSIDAD NACIONAL DE LA PLATA

Implementación de Preparación Forense para la continuidad digital

Tesista: Lic. Mónica Diana Tugnarelli.

Director: Lic. Francisco Javier Díaz

Tesis presentada para obtener el grado de
Magister en Redes de Datos

Facultad de Informática
Universidad Nacional de La Plata
Octubre 2019

Presentación de tesis

Una arquitectura de seguridad informática bien definida debe brindar un plan y un conjunto de políticas que describan tanto los servicios de seguridad ofrecidos a los usuarios como los componentes del sistema requeridos para implementar dichos servicios. Cuando se produce un incidente o amenaza de seguridad, en el cual un recurso del sistema queda comprometido o potencialmente expuesto a accesos no autorizados, esta arquitectura de seguridad se ve vulnerada.

Considerando la fragilidad y volatilidad de un evento digital, las técnicas y metodologías de forensia informática deben asegurar que se pueda determinar adecuadamente el *qué*, *quién, cuándo* y *cómo sucedió* el incidente de seguridad, así como también ocuparse de la correcta preservación de los datos que pueden recolectarse.

Frente a este desafío la metodología Forensic Readiness avanza hacia la protección de datos considerados evidencia digital desde el inicio, desde su selección como tal y aún antes de la posible ocurrencia de un incidente de seguridad informática.

Esta tesis de Maestría tiene por objetivo general realizar un análisis comparativo de modelos de implementación de dicha metodología, denominada también Preparación Forense, como una posible estrategia para la continuidad digital y la protección preventiva de los activos de una organización. Como objetivo específico el trabajo apunta a confeccionar un conjunto de Buenas Prácticas para la implementación de la metodología Forensic Readiness en una organización.

Para el logro de los objetivos, se analizaran las diversas etapas que sustentan esta metodología que propone que los datos se recolecten a priori de un incidente de seguridad y que se resguarden como posible evidencia digital buscando cumplir con dos objetivos primordiales: maximizar la capacidad del entorno para reunir evidencia digital confiable y minimizar el costo forense durante la respuesta a un incidente. Al respecto, la premisa es que esos datos puedan ser pasibles de ser utilizados no solo como insumo para el análisis de incidentes y como entorno de recuperación para la continuidad del negocio, sino también como prueba legal, lo que involucra el aseguramiento de la prueba a medida que se realiza la recolección activa de los datos.

Para efectuar un análisis comparativo adecuado de las prestaciones de este enfoque preventivo se lo contrastará con un enfoque reactivo, donde los datos se recolectan a posteriori de un incidente lo cual está más relacionado con las tareas de análisis forense y pericias informáticas sobre un evento consumado.

Desde el punto de vista práctico se configurará un entorno de prueba, se realizará un análisis de riesgo sobre activos identificados en una organización ficticia, se determinaran criterios y puntos de control sobre servidores web que implementan el protocolo HTTP en sus versiones 1.x y el reciente HTTP /2 y se simulará un ataque de Denegación de Servicio para capturar trafico a los fines de conocer el comportamiento del sistema y aspectos relacionados al resguardo de evidencia.

Durante los capítulos del trabajo se desarrollarán conceptos relacionados con seguridad digital, activos de información, evidencia digital, forensia informática, protocolos y metodologías para el análisis forense, aseguramiento de la evidencia y análisis de weblogs, para aportar desde lo técnico y lo académico, conclusiones generales y particulares acerca de la performance de los enfoques metodológicos de recolección, considerando aspectos tales como:

- La calidad de los datos recolectados.
- La trazabilidad de los datos.
- Nivel de disponibilidad de datos.
- Tiempos de respuesta ante incidentes.
- Resguardo de la evidencia.
- Relación entre continuidad digital y la disponibilidad forense.

Para finalizar este trabajo, se elaboraran conclusiones y posibles temas de desarrollo futuro en la temática.

CAPITULO 1. Incidentes de Seguridad Informática

1.1 Introducción

Los avances tecnológicos de los últimos años han causado una transformación digital que afecta transversalmente a todos los ámbitos de la vida. Estos avances, a la par de las mejoras que han traído aparejadas, también han expuesto a millones de dispositivos a potenciales incidentes de seguridad informática.

En la RFC 2828 [1] se define como un incidente de seguridad a un evento relevante para la seguridad, donde se desobedece o vulnera la política de seguridad poniendo en riesgo los recursos de una organización o sistema.

La política, documentada o no, de una organización especifica aspectos en relación a la clasificación de la información, la seguridad física y lógica de los datos y a los mecanismos de protección de activos, entre otros, tratando de detectar los requerimientos de los usuarios y gestionando de manera adecuada los recursos de toda la organización para dar servicios acordes a los objetivos primordiales del negocio.

Estas políticas no son estáticas, sino que deben ser revisadas con regularidad para garantizar su eficiencia y efectividad para enfrentar los desafíos tecnológicos y de seguridad actuales.

Al respecto, y considerando los últimos informes de empresas de renombre en el ámbito de la seguridad informática, la compañía Cisco, en su reporte semestral 2017 [2] detalla diversos riesgos de seguridad acentuando un escenario de actividades precursoras de un nuevo tipo de ataque centrado en la destrucción de servicios (DeOS), como así también los ataques de Denegación de Servicios sobre dispositivos de Internet de las Cosas (IoT).

El ESET Security Report 2018 [3] presenta el estado de la seguridad de la información en las empresas en Latinoamérica señalando que:

- Si bien tradicionalmente, el podio de preocupaciones de las empresas en la región estuvo liderado por los códigos maliciosos, el 2017 estuvo signado por la incidencia de ransomware (57%) y la variante Ransomware of Things (RoT) el cual resulta muy rentable para los atacantes. Por ello, resulta necesario proteger adecuadamente la información y otros activos de los códigos maliciosos de esta naturaleza.

- El criptojacking escala posiciones como amenaza detectada, producto de la "fiebre por las criptomonedas", donde los cibercriminales aprovechan esta situación desarrollando amenazas y provocando ataques para apropiarse de las monedas digitales, o bien, utilizando los recursos de cómputo de los usuarios de Internet, que de manera involuntaria contribuyen a la minería para beneficios de terceros.
- Un análisis de los datos recopilados evidencia que las infecciones con código malicioso afecta a las empresas de manera muy similar, sin importar su tamaño, aunque en las de mayor tamaño el porcentaje se eleva, aunque la explicación pueda hallarse probablemente en su capacidad para reconocer más fácilmente un incidente de este tipo, lo cual les deja margen para corregirlo. Por ende el porcentaje de pequeñas empresas que no cuentan con tecnologías de protección es más elevado que el que registran las empresas más grandes.
- Es importante resaltar que los engaños basados en ingeniería social han evolucionado a lo largo de los años logrando en muchos casos hacerse más efectivos. En el último tiempo han mutado desde simples sitios de phishing, hasta webs con certificados SSL falsos o gratuitos que explotan el desconocimiento del usuario de cara al funcionamiento del protocolo HTTPS, pasando por los ataques homográficos, que cada vez toman más relevancia registrando dominios que contienen malware suplantando empresas y marcas reconocidas,
- En cuanto a estrategias de defensa, solo un 58% de las empresas más pequeñas cuentan con una política de seguridad en contraposición al 78% de empresas grandes que sí cuentan con este tipo de controles.

Ya los reportes del tercer y cuarto trimestre de 2017 realizados por la empresa Karspesky [4] avizoraban la intensificación del número de ataques de Denegación Distribuida de Servicios (DDoS) proveniente de botnets conformadas por miles de dispositivos radicados en más de cien países que atacan no solo a sistemas, sino también a dispositivos móviles y a sitios que se dedican a las criptomonedas. En el análisis discriminado por tipo de incidentes, la proporción de ataques HTTP, protocolo de interés para este trabajo de tesis, aumentó del 7,27% al 11,6% convirtiéndose en el tercero en popularidad.

Debido al crecimiento en la incidencia, diversos países han avanzado en la identificación y procesamiento judicial de los responsables de la creación de botnets y organizadores de ataques DoS.

En el State of Cybersecurity 2018 [5] se informan los resultados de la encuesta mundial anual de ISACA sobre el estado del sector, los cuales confirman que la ciberseguridad sigue siendo dinámica y turbulenta a medida que el campo sigue en crecimiento. A medida que los ciberataques continúan amenazando a organizaciones de todo tipo y tamaño, se da prioridad crítica a la creación de equipos de expertos en ciberdefensa, señalándose el déficit de habilidades en la formación de recursos humanos en el área. Surgen nuevas técnicas y métodos de ataque, como el malware sin archivos, donde los atacantes toman herramientas que están incorporadas en Windows y las usan para llevar a cabo el ataque, y métodos tales como Meltdown y Spectre basados en fallos de diseño de los procesadores de Intel. Los ciberataques están aumentando, pero los métodos empleados se mantienen relativamente estáticos.

La mayoría de las empresas emplea alguna capacidad de inteligencia para la prevención de amenazas, a menudo con personal interno. Por otra parte, diversas estrategias de defensa activa, aunque no se extienden de manera masiva entre las empresas, han demostrado un alto nivel de éxito cuando se implementan.

En la figura 1 se muestra el resumen del relevamiento efectuado en 2018 en relación al incremento o disminución de ataques en comparación con 2017, destacándose que el 50% de las empresas consultadas registró una mayor cantidad de ataques y que el 18% de las organizaciones desconoce si los ha sufrido, lo cual posiblemente haya puesto en peligro a todos los activos de la organización.

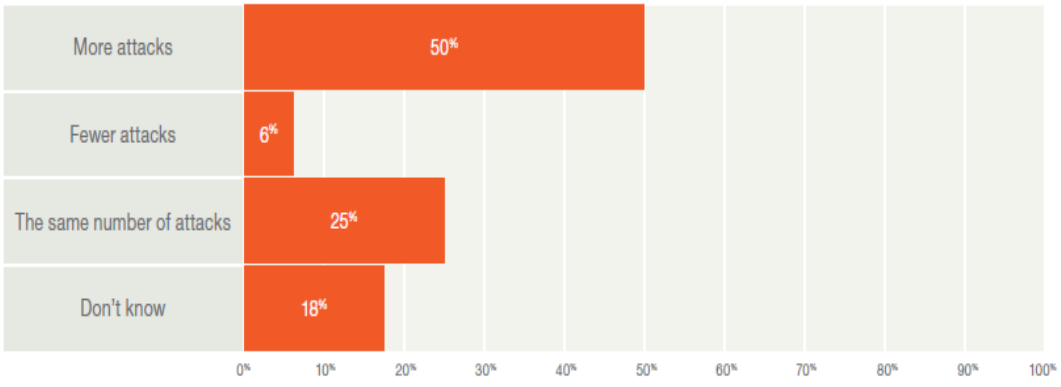

Fig 1. ISACA. Comparativa 2017-2018 en cantidad de ataques

Claramente la tendencia es en aumento, englobando diferentes ataques de seguridad a todo tipo de organizaciones.

Por su parte en el primer State of Cybersecurity 2019 de ISACA [6] , se remarca de manera enfática que los ataques se incrementan pero que aún las organizaciones destinan un bajo

presupuesto para seguridad informática y que los profesionales especialistas en el tema son drásticamente escasos para el extenso campo laboral que se presenta.

Este breve resumen de reportes muestra el crecimiento acelerado de la ciberdelincuencia en consonancia con la creación, utilización e integración de tecnologías, llegando al punto en que cada producto o innovación tecnológica puede ser tomado como una base para el desarrollo de vectores de ataques.

Si a todo esto se suma la ocurrencia de incidentes de seguridad internos a la organización se presenta un escenario complejo que obliga a pensar en una política de seguridad de la información desde el diseño del modelo, con mecanismos y estrategias de prevención de incidentes que proporcionen una arquitectura de seguridad correctamente definida para ofrecer un plan y un conjunto de políticas que describan tanto los servicios de seguridad ofrecidos a los usuarios como los componentes del sistema requeridos para implementarlos.

En este punto el reto no solo pasa por disponer de personal calificado en las áreas de seguridad, sino también porque la organización cuente con un modelo de seguridad simple e integrado para aumentar la capacidad de enfrentar los riesgos y retos. La mayoría de las organizaciones no cuenta con estrategias de protección de activos ni con planes de contingencias que establezcan como reconstruir toda su tecnología e información desde cero, por lo que esta debilidad solo expande el escenario de riesgo.

Es importante para la continuidad del negocio que cada organización tenga bien definida la política de seguridad que aplica a los activos de información que han sido identificados por su relevancia y relación con los objetivos de la misma, conociendo como se gestionan y cuáles son sus riesgos para implementar mecanismos que aseguren la confidencialidad, la integridad, la disponibilidad de dichos activos y la trazabilidad de los datos.

Esa trazabilidad de datos debe ser entendida no solo como el aseguramiento de una fácil localización de datos y errores para simplificar su corrección, sino también que es una actividad que debe ajustarse a normativas legales vigentes ayudando a mantener el control sobre los tratamientos que se realizan sobre esos datos que son el activo esencial de cualquier organización. Sin la cadena de trazabilidad que asegure una buena gestión de datos se perdería gran parte de la utilidad de los mismos.

En este entorno tecnológico las metodologías de forensia informática deben asegurar que se pueda determinar adecuadamente el qué, quién, cuándo y cómo sucedió en relación a ese incidente de seguridad, así como también ocuparse de la correcta preservación de los datos recolectados.

1.2 Forensia Informática

La definición brindada por el Digital Forensics Research Workshop (DFRWS), acuerda que el análisis forense digital o forensia informática es "*El uso de métodos científicamente probados y derivados hacia la preservación, recolección, validación, identificación, análisis, interpretación, documentación y presentación de evidencia digital derivada de fuentes digitales con el fin de facilitar o promover la reconstrucción de los hechos, que pueden constituirse en evidencia legal, o ayudando a anticipar acciones no autorizadas que han demostrado ser perjudiciales para operaciones planeadas*."

Por su parte, Kovacich define a la Informática Forense como la aplicación legal de métodos, protocolos y técnicas para obtener, analizar y preservar evidencia digital relevante a una situación en investigación. [7]

Para el FBI, Federal Bureau of Investigation (FBI), principal agencia de investigación criminal del Departamento de Justicia de Estados Unidos, la informática (o computación) forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional, procurando identificar a los autores, los procesos involucrados y aquellos que llevaron a tener el incidente de seguridad [8].

Desde el punto de vista estructural, la informática forense debe apuntar en dos direcciones:

- hacia adentro de la organización para clarificar y documentar procesos erróneos y para determinar responsabilidades internas y;
- hacia el exterior para constituir prueba de validez legal para perseguir a los autores de los incidentes.

Así, la informática forense se presenta como una disciplina, no solo auxiliar de la justicia, sino como aliada necesaria para enfrentar los desafíos de la seguridad informática moderna. Requiere de una correcta aplicación de métodos científicos, técnicas y herramientas para cumplimentar las etapas relacionadas con la identificación, preservación y análisis de la evidencia digital la cual, llegado el caso, puede ser considerada legalmente en un proceso judicial por lo que además se necesita cerciorar la calidad y trazabilidad de estos datos para asegurar su admisibilidad.

Para los datos considerados evidencia se debe preservar una cadena de custodia, concepto similar a lo utilizado para evidencias físicas, la cual es el procedimiento controlado que se aplica a los indicios materiales relacionados con el delito, desde su localización hasta su valoración por los encargados de administrar justicia y que tiene

como fin no viciar el manejo de que ellos se haga y así evitar alteraciones, sustituciones, contaminaciones o destrucciones [9].

El Código Procesal Penal de la Nación Argentina [10] en su artículo 150 establece que "*con el fin de asegurar los elementos de prueba, se establecerá una cadena de custodia que resguardará su identidad, estado y conservación. Se identificará a todas las personas que hayan tomado contacto con esos elementos, siendo responsables los funcionarios públicos y particulares intervinientes*".

Este punto se complementa con la documentación detallada de los procedimientos, herramientas y resultados sobre los sistemas informáticos analizados. El investigador debe custodiar su propio proceso de forensia de manera de que todo lo realizado, y la evidencia recolectada, tenga carácter de indubitable.

Diversas herramientas y aplicaciones de forensia asisten al investigador en este proceso existiendo en el mercado numerosas herramientas de código abierto y otras de código propietario. En este trabajo, tanto para el entorno de prueba como las herramientas de forensia utilizadas, son open source y las actividades se realizaron usando Ethical Hacking como enfoque metodológico en un ambiente real, académico y controlado.

1.3 Activos de información

Para un correcto diseño y aplicación de estrategias de seguridad informática en una organización, factores que además están estrechamente relacionados con la dimensión de una política de seguridad, es preciso que puedan identificarse los activos que son imprescindibles para el cumplimiento de los objetivos de la propia organización.

Una organización, cualquiera sea su tipo, posee información crítica que desea proteger frente a cualquier situación que suponga un riesgo o amenaza. Esta información que resulta fundamental para la organización se denomina un activo de información.

La norma española UNE (UNE 71504:2008) [11], considerada en varias metodologías de análisis y gestión de riesgos, amplía esta definición estableciendo que: *un activo de la organización es un componente, funcionalidad o servicio de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización*.

Así, como ejemplos de activos se pueden considerar a las bases de datos, archivos, documentación del sistema, contratos informáticos, software del sistema y aplicaciones que dan servicio a la organización, recursos humanos, el hardware y todo lo que compone la estructura organizacional. Incluso la información al tener diferentes grados de

sensibilidad y criticidad, puede ser clasificada para definir un conjunto apropiado de niveles de protección.

La norma ISO/IEC 27002 [12] establece un marco para la gestión de activos, que comprende desde la identificación del activo hasta la definición de las responsabilidades de la protección adecuada para el mismo.

Además, recomienda contar con un inventario con la correspondiente identificación de activos y su nivel de importancia. Este inventario debe incluir toda la información necesaria para poder recuperarse frente a un desastre, incluyendo el tipo de activo, formato, ubicación de la copia de seguridad y su valor para el negocio.

Este estándar define diferentes tipos de activos, que incluyen

a) Información, bases de datos, archivos, contratos y acuerdos, documentación de sistemas, manuales de usuario, planes para la continuidad del negocio y pistas de auditoría.
b) Archivos de software, software de aplicaciones, software de sistemas, herramientas de desarrollo y utilitarios.
c) Activos físicos, tales como equipamiento de computación y de comunicaciones.
d) Servicios de computo y comunicaciones
e) Activos intangibles tales como la reputación y la imagen de la empresa

Con una adecuada aplicación de métodos de gestión de riesgos se puede realizar un análisis para determinar tanto los activos más relevantes para una organización como las amenazas a las que están expuestos y el impacto (y costo) de las mismas en caso de que ocurran. La construcción de escalas valorativas, cuantitativas y cualitativas, pueden responder a preguntar esenciales, como por ejemplo:

- *¿Cuánto tiempo puede estar la organización sin el activo en modo operativo?*
- *¿Qué tiempo promedio se requiere para la recuperación del activo ante la ocurrencia de un incidente?*
- *¿Qué costos implica la recuperación del activo?*

Y con relación a tres requisitos básicos de seguridad:

- ***Confidencialidad****: ¿qué daño causaría que el activo pueda ser accedido por entes no autorizados?*
- ***Integridad****: ¿qué perjuicio causaría su daño o corrupción?*
- ***Disponibilidad****: ¿qué inconveniente causaría no tener o no poder utilizarlo?*

Varios de estos conceptos se retomarán en el capítulo 6 de este trabajo donde se presenta un caso práctico de identificación y protección de activos utilizando Magerit Versión 3

[13], una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España que ofrece un método sistemático para analizar los riesgos derivados del uso de TICs y para implementar medidas de control adecuadas que permitan identificar y mitigar riesgos.

Magerit puede usarse en combinación con otras normas y marcos de trabajo para la gestión de riesgos de seguridad, tales como ISO 27000 y 31000, integrándose en la etapa de implementación de la gestión de riesgos. Se ha seleccionado para este trabajo debido a que es una metodología de carácter público y que puede ser utilizada libremente por cualquier tipo de organización.

CAPITULO 2. Estándares y modelos aplicables a la recolección de evidencia digital

2.1 Introducción

Uno de los aspectos más importantes de la forensia informática es la metodología utilizada para recolectar y preservar la evidencia digital, que si bien en muchos aspectos es como cualquier otra evidencia, tiene características distintivas que requieren de procesos especiales para su recolección y gestión.

Se deben considerar cuestiones tales como: la preparación de los sistemas para crear y resguardar registros electrónicos; el gran volumen de estos y las necesidades de almacenamiento fiable; los registros originales que deben diferenciarse explícitamente de sus copias; la volatilidad que los hace pasible de ser alterados y borrados; y la adecuada implementación de una cadena de custodia que permita la trazabilidad de los registros.

En este capítulo se presentan conceptos relacionados y una selección de los estándares y documentos más ampliamente utilizados como soporte normativo para la recopilación y tratamiento de la evidencia digital.

2.2 Evidencia digital

Según define el *HB: 171 2003 Guidelines for the Management of IT Evidence* [14], la evidencia digital es "*… cualquier información que, sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático…*", por lo que, y en términos generales, evidencia digital se puede utilizar para describir cualquier registro generado por o almacenado en un sistema informático o dispositivo digital que pueda ser utilizado como prueba en un proceso legal. De manera aun más abarcativa, Eoghan Casey [15] define a la evidencia digital como "*cualquier dato que puede indicar que un crimen ha sucedido o que pueda proporcionar un enlace entre un crimen y su víctima o un crimen y su autor*".

Casey resalta también el carácter ubicuo de las computadoras y los distintos canales de transmisión de datos, todos ellos fuente de evidencia digital con diversas características. Acorde a esto propone, una categorización de los sistemas informáticos en tres grupos:

- Sistemas informáticos abiertos: son computadoras de trabajo, sistemas compuestos de discos, teclados, etc. Estos sistemas, con su cantidad cada vez mayor de espacio de almacenamiento, pueden ser generosas fuentes de evidencia digital. Un simple archivo puede contener información incriminatoria y puede tener propiedades asociadas que son útiles en una investigación. Por ejemplo, detalles como cuándo se creó un archivo, quién lo creó o si se creó en otra computadora pueden ser datos de importancia.
- Sistemas de comunicaciones: Sistemas telefónicos, sistemas inalámbricos, Internet y las redes en general son fuente de evidencia digital. Por ejemplo, cuando se envía un mensaje de correo electrónico, diversos protocolos usados en internet lo transporta hasta el sistema destino. La marca de tiempo del mensaje, quien lo envió y el contenido pueden ser importantes en la investigación, Pero también, para verificar cuando se envió el mensaje es necesario examinar los archivos *log* de servidores y routers intermedios por los que ha pasado el mensaje.
- Sistemas embebidos: dispositivos móviles, tarjetas de memoria y cualquier otro sistema embebido puede contener evidencia digital, como por ejemplo un teléfono celular puede contener comunicaciones, archivos, fotos y otro tipo de datos personales, los sistemas de navegación pueden usarse para localizar un vehículo pero también para conocer donde ha estado y diversos electrodomésticos pueden descargar información desde internet y también utilizarse de modo remoto mediante aplicaciones de usuarios.

Es evidente que las fuentes digitales proveedoras de los datos a analizar son numerosas, abarcan todo tipo de dispositivos y tienen diferentes formatos. Estas son algunas de las causas por las que se hace necesario que el análisis forense digital aplique métodos científicos, técnicas y herramientas para cumplimentar etapas relacionadas con la identificación, preservación y análisis de la evidencia digital.

El documento *HB*: *171* citado anteriormente, determina que la evidencia digital puede ser dividida en tres categorías:

a- Registros almacenados en un dispositivo (ejemplo: archivos, correos electrónicos)

b- Registros generados por los dispositivos (ejemplo: registros de eventos, de transacciones, de auditoría)

c- Registros que han sido parcialmente generados y almacenados en el dispositivo informático (ejemplo: consultas a bases de datos, documentos, hojas de cálculo)

De acuerdo con la ISO/IEC 27037:2012 [16] la evidencia digital es gobernada por tres principios fundamentales: la relevancia, la confiabilidad y la suficiencia, entendiéndose como tales lo siguiente:

- **Relevancia**: la evidencia digital debe estar relacionada con los hechos investigados
- **Confiabilidad**: la evidencia debe ser repetible y auditable, de tal manera que un tercero que aplique el mismo método utilizado llegue al mismo resultado
- **Suficiencia**: la evidencia recolectada debe ser suficiente para sustentar los hallazgos obtenidos por el analista forense

Para el cumplimiento de estos requisitos se requieren de procesos, metodologías, técnicas, herramientas y habilidades profesionales especiales en la gestión de evidencia TI que se presentarán en puntos posteriores de este trabajo.

La evidencia digital, entonces, se convierte en un insumo primario para cualquier investigación forense, y por su carácter preponderadamente volátil debe contemplar aspectos básicos en cuanto a su recolección, almacenamiento, trazabilidad, mantenimiento de la cadena de custodia, resguardo e indubitabilidad de la misma.

2.3 Estándares y modelos

Como marco general para este trabajo de tesis se analizaron los estándares y modelos más ampliamente difundidos, tales como la RFC 3227 [17] que especifica las "*Directrices para la recopilación de evidencias y su almacenamiento*" y la ISO/IEC 27037 "*Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*" que actualiza las directrices establecidas en la RFC citada anteriormente. Ambas normas plantean un conjunto de puntos comunes para realizar un análisis forense correcto, entre ellos los siguientes:

- La importancia de preservar el entorno de pruebas,
- Cómo y donde se guardan las pruebas,
- Cómo se analizan para obtener el máximo rendimiento y,

- La importancia de que los informes sean claros y concisos.

Asimismo en este trabajo, se examinaron documentos que plantean buenas prácticas en el manejo de la evidencia digital, tales como:

1. *HB: 171 2003 Guidelines for the Management of IT Evidence* de la Standards Australia International,
2. *Guide to Integrating Forensic Techniques into Incident Response del* NIST: National Institute of Standards and Technology [18]
3. *Guía de Obtención, Preservación y Tratamiento de Evidencia Digital*, acordada por los Ministerios Públicos del MERCOSUR [19]

A continuación se describen las principales características de las normativas y documentos citados.

2.3.1 RFC-3227: Directrices para la recolección de evidencias y su almacenamiento

El RFC 3227 de la Internet Engineering Task Force (IETF) es un documento, publicado en 2002, que describe directrices para la recopilación de información relacionada a incidentes de seguridad e intrusiones y a su posterior almacenamiento. Puede considerarse un estándar de facto, de carácter orientativo para administradores de sistemas.

Este documento especifica que, si la recolección de evidencia se hace correctamente es mucho más útil y se logra más rapidez en encontrar al atacante y, a la vez, se cuenta con más posibilidades de que la evidencia digital se admita como prueba legal en caso de ser requerida como tal.

Los puntos más importantes de la RFC 3227 establecen principios, procedimientos y herramientas necesarias a tener en cuenta, como por ejemplo se recomienda:

- Durante la recolección de evidencias

- Cumplir con la política de seguridad establecida y dar participación al personal capacitado en manejo de incidentes y en aspectos legales.
- Capturar una imagen del sistema tan precisa como sea viable.
- El procedimiento de recolección debe ser lo más detallado posible, procurando que no sea ambiguo y reduciendo al mínimo la toma de decisiones, por lo cual se deben realizar notas pormenorizadas, incluyendo fechas y horas en cada captura y en cada reporte. Cada documento debe estar firmado, fechado y ser lo

suficientemente descriptivo para servir como base de una declaración ante la justicia.

- Minimizar los cambios en la información que se está recolectando y eliminar los agentes externos que puedan hacerlo.
- En el caso de enfrentarse a un dilema entre recolección y análisis elegir primero recolección y después análisis.
- Recoger la información según el orden de volatilidad. Se recomienda recolectar en primer lugar aquella información que vaya a estar disponible durante el menor período de tiempo, es decir, aquella cuya volatilidad sea mayor. De acuerdo a esta escala se puede crear la siguiente lista ejemplo en orden de mayor a menor volatilidad:
    - Registros y contenido de la caché.
    - Tabla de enrutamiento, caché ARP, tabla de procesos, estadísticas del kernel, memoria.
    - Información temporal del sistema.
    - Disco
    - Logs del sistema.
    - Configuración física y topología de la red.
    - Documentos.

- Los métodos utilizados para recolectar evidencias deben ser transparentes y reproducibles. Se debe estar preparado para reproducir con precisión los métodos usados, y que dichos métodos hayan sido testados por expertos independientes.
- La cadena de custodia debe estar claramente documentada y con un registro detallado de los siguientes puntos y cualquier modificación sobre los mismos:
    - *¿Dónde?, ¿cuándo? y ¿quién? descubrió y recolectó la evidencia.*
    - *¿Dónde?, ¿cuándo? y ¿quién? manejó la evidencia.*
    - *¿Quién ha custodiado la evidencia?, ¿cuánto tiempo? y ¿cómo la ha almacenado?*

- Acciones que deben evitarse

Se debe evitar cualquier acción que pueda invalidar el proceso de recolección de información ya que debe preservarse su integridad con el fin de que los resultados obtenidos puedan ser utilizados en un proceso judicial en el caso de que sea necesario. Al respecto, citando algunas, se recomienda: no apagar el dispositivo

hasta que se haya recopilado toda la información, se debe recopilar la información mediante programas desde un medio protegido, no ejecutar programas que modifiquen la fecha y hora de acceso de todos los archivos del sistema y si es necesario solicitar una autorización por escrito de quien corresponda para llevar a cabo la recolección de evidencias, ya que puede darse el caso de que se trabaje con información confidencial.

2.3.2 ISO/IEC 27037:2012 Information technology. Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence

Considerando el marco normativo dado por la ISO/IEC 27001, donde se definen los requisitos de un Sistema de Gestión de la Seguridad de la Información, con el complemento dado por la 27002, que es una guía de buenas prácticas para aplicar en cuanto a seguridad de la información, la norma 27037 aborda de manera específica pautas para la identificación, recolección, adquisición y preservación de la evidencia digital con vista a tres principios fundamentales: la relevancia, la confiabilidad y la suficiencia. Estos tres elementos definen la formalidad de cualquier investigación basada en evidencia digital, ya sea que esta se utilice para que sea admisible en una corte de justicia o no.

Este estándar proporciona orientación y directrices destinadas a los responsables DEFR´s (*Digital Evidence First Responders*) y DES´s (*Digital Evidence Specialist*) para actividades relacionadas con el manejo de la potencial evidencia digital en todas sus etapas: identificación, adquisición y preservación. Claramente esta norma está dirigida a la actuación pericial, no al análisis de la evidencia digital. En coincidencia con la RFC 3227 especifica recomendaciones básicas tales como:

- La evidencia digital debe ser adquirida del modo menos intrusivo posible tratando de preservar la originalidad de la prueba y en la medida de lo posible obteniendo copias de respaldo.
- Los procedimientos seguidos y la documentación generada deben haber sido validados y contrastados por las buenas prácticas profesionales. Se debe proporcionar trazas y evidencias de lo realizado y sus resultados.
- Los métodos y procedimientos aplicados deben de ser reproducibles, verificables y argumentables al nivel de comprensión de los entendidos en la materia, quienes puedan dar validez y respaldo a las actuaciones realizadas.

- Las herramientas utilizadas deben de ser mencionadas y éstas deben de haber sido validadas y contrastadas en su uso para el fin en el cual se utilizan en la actuación.
- Para cada tipología de dispositivo la norma divide la actuación o su tratamiento en tres procesos diferenciados como modelo genérico de tratamiento de las evidencias:
    - **Identificación**: Es el proceso de la identificación de la evidencia y consiste en localizar e identificar las potenciales informaciones o elementos de prueba en sus dos posibles estados, el físico y el lógico según sea el caso de cada evidencia.
    - **Recolección/Adquisición**: Este proceso se define como la recolección de los dispositivos y la documentación (incautación y secuestro de los mismos) que puedan contener la evidencia que se desea recopilar o bien la adquisición y copia de la información existente en los dispositivos.
    - **Conservación**: La evidencia ha de ser preservada para garantizar su utilidad, es decir, su originalidad para que a posteriori pueda ser ésta admisible como elemento de prueba original e íntegra, por lo tanto, las acciones de este proceso están claramente dirigidas a conservar la Cadena de Custodia, la integridad y la originalidad de la prueba.

Un aspecto relevante a considerar es que la aplicación de un estándar internacional, requiere del estricto cumplimiento de las leyes nacionales, códigos, normas y regulaciones específicos para cada país.

2.3.3 Standard Australia International: HB: 171 2003 Guidelines for the Management of IT Evidence

Este estándar tiene como principal objetivo proporcionar orientación sobre la gestión de registros electrónicos que pueden ser utilizados como evidencia en procedimientos judiciales o administrativos, o cuando una actividad delictiva es sospechosa y deben recolectarse pruebas para investigación.

El manual define la evidencia TI como: "*cualquier información, ya sea sujeto a intervención humana o de otro tipo, que se haya extraído de una computadora. La evidencia de TI debe estar en una forma legible para el hombre o ser interpretada por*

personas que tengan experiencia en la presentación de dicha información con la ayuda de un programa de computadora".

Si bien la guía puede aplicarse a cualquier evidencia electrónica, el enfoque del manual se centra en las pruebas relacionadas con la informática, incluidas las comunicaciones informáticas, propendiendo a que los especialistas en informática forense puedan encontrar el equilibrio aceptable entre la tecnología y la ley, es decir que la prueba legal se correlacione lo más posible con la prueba científica.

La gestión de la evidencia de TI es una práctica interdisciplinaria, hay una serie de principios generales que pueden aplicarse para guiar a los profesionales a medida que aplican los conocimientos y la experiencia de su propio dominio para resolver problemas específicos, los cuales se detallan a continuación:

- <u>Obligación de proporcionar registros</u>

  a) Comprender las obligaciones reglamentarias, administrativas y de mejores prácticas de producir, conservar y proporcionar registros;

  b) Comprender los pasos que se pueden dar para maximizar el peso probatorio de los registros y las implicaciones de no hacerlo; y

  c) Comprender las restricciones reglamentarias a la conservación y suministro de registros

- <u>Diseño para la obtención de pruebas</u>

  Asegurarse de que los sistemas y procedimientos informáticos son capaces de establecer lo siguiente:

  a) La autenticidad y la modificación de los registros electrónicos
  b) La fiabilidad de los programas informáticos que generan dichos registros;
  c) La hora y la fecha de creación o modificación;
  d) La identidad del autor de un registro electrónico; y
  e) La custodia y el manejo seguro de los registros.

- <u>Recopilación de pruebas</u>

  Recopilar información de prueba asegurándose de que los procedimientos sean:

  a) tecnológicamente sólidos para recopilar todas las pruebas pertinentes; y

b) legalmente sólidos para maximizar la ponderación de las pruebas;

- Custodia de los registros
  a) Establecer procedimientos para la custodia y retención seguras de los registros probatorios;
  b) Mantener un registro que consigne todo el acceso a los registros probatorios y el manejo de los mismos; y
  c) Determinar si se está manipulando el registro original o una copia. La evidencia original debe ser preservada en el estado en el que fue identificada por primera vez - no debe ser alterada, y en los casos en los que la alteración es inevitable, entonces cualquier cambio debe ser documentado apropiadamente.

- Personal

  Asegurarse de que el personal involucrado en el diseño, producción, recolección, análisis y presentación de la evidencia tenga la capacitación, experiencia y calificaciones apropiadas para cumplir con su función.

El documento presenta el "Ciclo de vida de la gestión de las pruebas de TI" que se ilustra en la figura 2. El ciclo de vida trata de representar la idea de que la informática forense es un proceso activo y no una actividad post-mortem. Las organizaciones requieren de políticas de seguridad que contemplen las diferentes etapas de la evidencia digital, su tratamiento y resguardo de manera recursiva y continua.
El paso 6 de este gráfico expone el concepto de *Determinar el peso de la evidencia*, el cual representa el grado en que la evidencia representa a los hechos, en cuanto a su calidad y totalidad independientemente de su admisibilidad.

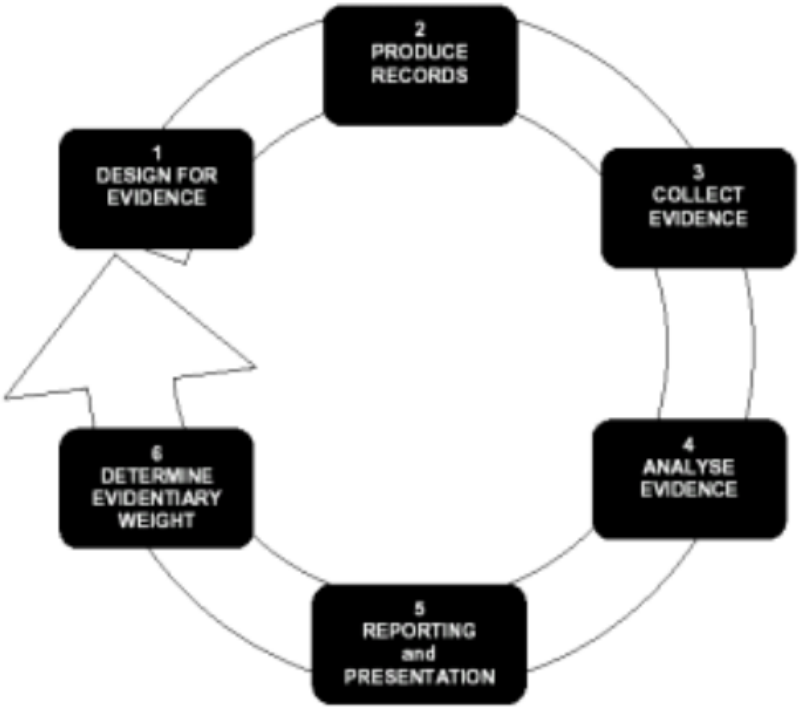

Fig.2 - HB: 171/2003 Ciclo de vida de la gestión de las pruebas de TI

2.3.4 National Institute of Standards and Technology (NIST). Guide to Integrating Forensic Techniques into Incident Response.

Al igual que las anteriores esta guía coincide en los aspectos principales del uso de las técnicas forenses para resguardo de evidencia, su importancia en la reconstrucción de incidentes de seguridad y la capacidad que deben tener todas las organizaciones para enfrentar este desafío. Sin tal capacidad, una organización tendrá dificultades para determinar qué eventos han ocurrido dentro de sus sistemas y redes, y si datos confidenciales han sido expuestos.

La guía proporciona información detallada sobre el establecimiento de una capacidad forense, incluido el desarrollo de políticas y procedimientos. Se enfoca principalmente en el uso de técnicas forenses para ayudar con la respuesta a incidentes de seguridad informática, pero gran parte del material también es aplicable a otras situaciones.

El proceso para realizar análisis forenses digitales comprende las siguientes fases básicas:

- **Recolección**: identificación, etiquetado, registro y adquisición de datos de las posibles fuentes, mientras se siguen procedimientos que preservan la integridad de los datos.
- **Examen:** procesamiento forense de los datos recopilados combinando métodos automatizados y manuales, y la evaluación y extracción de datos de interés particular, al tiempo que se preserva la integridad de los mismos.
- **Análisis**: analizar los resultados del examen utilizando métodos y técnicas legalmente justificables, para obtener información útil que responda a las preguntas que fueron el impulso para realizar la recopilación y el examen.
- **Informe**: informe de los resultados del análisis, que puede incluir la descripción de las acciones utilizadas, una explicación de cómo se seleccionaron las herramientas y los procedimientos, la determinación de qué otras acciones deben realizarse y proporcionar recomendaciones para mejorar las políticas, procedimientos, herramientas y otros aspectos del proceso forense.

El documento hace hincapié en la necesidad de implementar una política de seguridad en la organización, la cual debe incluir declaraciones específicas que aborden las principales consideraciones y procedimientos forenses, en el marco de las leyes y regulaciones aplicables, así como también indicaciones para su revisión periódica

En lo particular la guía presenta al análisis forense desde un enfoque de TI y no desde el cumplimiento de una ley, la publicación describe los procesos para realizar actividades forenses efectivas a la vez que brinda asesoramiento dirigido principalmente a equipos de respuesta a incidentes; analistas forenses; administradores de sistemas, redes y seguridad.

2.3.5 Acordada Ministerios Públicos del MERCOSUR. Guía de Obtención, Preservación y Tratamiento de Evidencia Digital

Este instrumento fue presentado y aprobado en el marco de la XVII Reunión Especializada de Ministerios Públicos del Mercosur, celebrada en Buenos Aires en noviembre de 2014. El trabajo señala una serie de herramientas de investigación como forma de reforzar la actividad del Ministerio Público Fiscal en los casos en que se cuente con evidencia digital. Concretamente, aborda el modo en el cual se debe obtener, conservar y tratar la evidencia digital para mejorar los niveles de eficiencia en

materia de persecución penal, en tanto resulta ser un eje central de preocupación de la comunidad internacional para la investigación transfronteriza del delito. La guía repasa diferentes documentos internacionales que dan cuenta de la relevancia a nivel mundial del fenómeno de la cibercriminalidad.

Particularmente aborda lo relativo a la obtención, conservación y tratamiento de la evidencia digital como base para asegurar el éxito de las investigaciones de numerosos delitos, proponiendo recomendaciones basadas en las utilizadas a nivel mundial para incautar, analizar y preservar la evidencia digital las que deben ser tenidas en cuenta por los operadores judiciales.

En relación se presentan principios generales y específicos para la recolección y preservación de la evidencia digital, con indicaciones para el embalaje, traslado y resguardo de la evidencia digital, la manipulación idónea del hardware, la forma adecuada de realizar una imagen o copia forense y como aplicar el hash para resguardo de la integridad.

Los principios acordados son los siguientes:

- Al llegar a la escena donde se va a obtener evidencia digital, lo primero que debe hacerse es evitar su contaminación, retirando del lugar a toda persona ajena al procedimiento que se está llevando a cabo;
- En segundo lugar, ninguna acción de las fuerzas de seguridad o de sus agentes debe alterar los datos contenidos en las computadoras o dispositivos de almacenamiento informático que luego serán utilizados como elementos de prueba;
- Si las circunstancias del caso hacen necesario que se deba acceder a los datos o información contenida en las computadoras o dispositivos de almacenamiento informático, la persona que efectúe dicha tarea debe ser idónea, es decir, contar con los conocimientos técnicos informáticos que la situación merece y, a su vez, ser capaz de explicar el motivo por el cual debió interactuar con la evidencia digital y los pasos cumplidos;
- Finalmente, se debe auditar y registrar fehacientemente todo el proceso relativo a la manipulación de la evidencia digital, precisando detalladamente las medidas y acciones llevadas a cabo, teniendo como eje central, la preservación de la cadena de custodia

Este documento en común también conviene una definición de evidencia digital, conceptuándola como "… *el conjunto de datos e información relevantes para una*

investigación, que se encuentra almacenada en o es transmitida por una computadora o dispositivo electrónico…", destacando la volatilidad de esta evidencia lo que le otorga una naturaleza frágil, fácil de alterar, dañar o destruir.

Si bien esta guía no es exhaustiva, puede considerarse un avance como iniciativa a ser aplicada en las fiscalías del poder judicial argentino.

Por estar relacionado con lo citado anteriormente se agrega a este punto que, en el marco del proyecto" Justicia 2020" impulsado por el Ministerio de Justicia y Derechos Humanos de la Nación Argentina [20] , se han presentado propuestas de actualización del Código Procesal Penal en materia de informática jurídica y criminalística digital. Se contempla el ajuste de la normativa en materia de evidencia digital o electrónica como elemento probatorio y las especificidades para su obtención y admisión a sabiendas de que la misma requiere de métodos específicos, métodos de preservación especiales y tratamiento criminalístico particular.

A modo de conclusión, los estándares y guías presentados en este capítulo si bien presentan ciertas diferencias en sus métodos y herramientas aplicables al proceso de forensia, coinciden en aspectos sustanciales a la hora de enfrentar una investigación forense, en cuanto al tratamiento de la evidencia digital con sus características particulares y a la necesidad de contar con recursos humanos capacitados para llevar adelante la tarea.

CAPITULO 3. Metodologías de recolección de datos digitales. Forensic Readiness

3.1 Introducción

En el capítulo anterior se describieron las normativas y documentos que hacen referencia al tratamiento de la evidencia digital las cuales dan un marco de actuación para su obtención y preservación y que han sido seleccionadas para este trabajo de tesis. Existen otras guías de buenas prácticas para el tema y también otros estándares con aplicación en diversos países, lo importante es la coincidencia de todos en el objetivo primordial de preservar la evidencia para que pueda ser usada en una investigación forense.

La siguiente cuestión que se pone en discusión es determinar en qué momento conviene realizar la recolección de evidencia para su correcto aseguramiento y para un adecuado análisis forense, es decir, determinar si:

¿Se obtiene la evidencia después de la ocurrencia de un evento de inseguridad?

¿Se puede resguardar la posible evidencia antes de que ocurra un incidente?

¿La organización está preparada para resguardar la evidencia?

¿Qué impacto tiene sobre la forensia digital el obtener los datos luego del incidente o tenerlos antes de la ocurrencia del mismo?

Para empezar a responder estos interrogantes, en este capítulo se abordará el análisis de dos enfoques los cuales tienen características comparativas y distintivas que permitirán identificar sus prestaciones en cuanto al tiempo de recolección y posterior tratamiento de datos considerados como evidencia digital, interna o externa, pero ambas susceptibles de ser usadas en un proceso judicial.

3.2 Enfoques de recolección de datos

Según el momento de detección de un incidente de seguridad, se pueden determinar dos enfoques de recolección y tratamiento de la evidencia digital [21], a saber:

a) Enfoque reactivo luego de ocurrido el incidente y,

b) Enfoque preventivo, antes de la ocurrencia del incidente.

A continuación se describen las principales características y prestaciones de cada uno de ellos:

3.2.1 Enfoque reactivo - Recolección de datos a posteriori de un evento de seguridad.

En este enfoque se trata de recuperar la evidencia luego de detectarse el incidente de seguridad y sobre todo como una respuesta al mismo, con el objetivo principal de realizar un análisis forense para determinar lo ocurrido cuando, por ejemplo, se detecta un acceso indebido en una computadora, se hace la imagen de disco y la investigación forense trata de localizar los rastros de evidencia en esa copia.

Sin importar el tipo de dispositivo, esta investigación debe ser realizada empleando un método sistemático, estandarizado y que contemple aspectos legales para asegurar la admisibilidad como prueba de la evidencia recolectada, sin olvidar que el proceso de una investigación forense digital está sujeto a un escrutinio considerable tanto de la integridad de la evidencia [Sommer 1998], como de la integridad del proceso de investigación [Stephenson 2002, 2003b].

En este tipo de procedimiento, las etapas que se pueden aplicar en todos los casos periciales en los que intervengan elementos vinculados a la informática, incluyen:

- el estudio y análisis del entorno, para identificar la evidencia digital a obtener;
- el análisis de los puntos de pericia, que establecen el objetivo que debe cumplir la evidencia digital;
- la adquisición de la evidencia digital;
- el análisis de la evidencia obtenida, conforme a los lineamientos del cuestionario pericial ordenado;
- la forma de exponer la evidencia digital obtenida en la investigación realizada;
- la preservación de la evidencia digital para eventuales futuras etapas de investigación, cuya fuente sería la misma evidencia digital.

En la Tesis Doctoral *Protocolos a aplicar en la forensia informática en el marco de las nuevas tecnologías (Pericia- Forensia y Cibercrimen)* [22] Piccirilli propone un protocolo pericial y forense de actuación de seis etapas que incluye los aspectos descriptos anteriormente, partiendo de la intervención del poder judicial que indica los requerimientos específicos relacionado con la evidencia según el tipo de delito que está bajo investigación, la extracción de evidencia digital, las herramientas a aplicar, el

resguardo adecuado, el análisis de los diversos reportes y su posterior elevación al tribunal correspondiente.

En el siguiente cuadro se muestran las diferentes etapas con los puntos a cumplir en cada una de ellas:

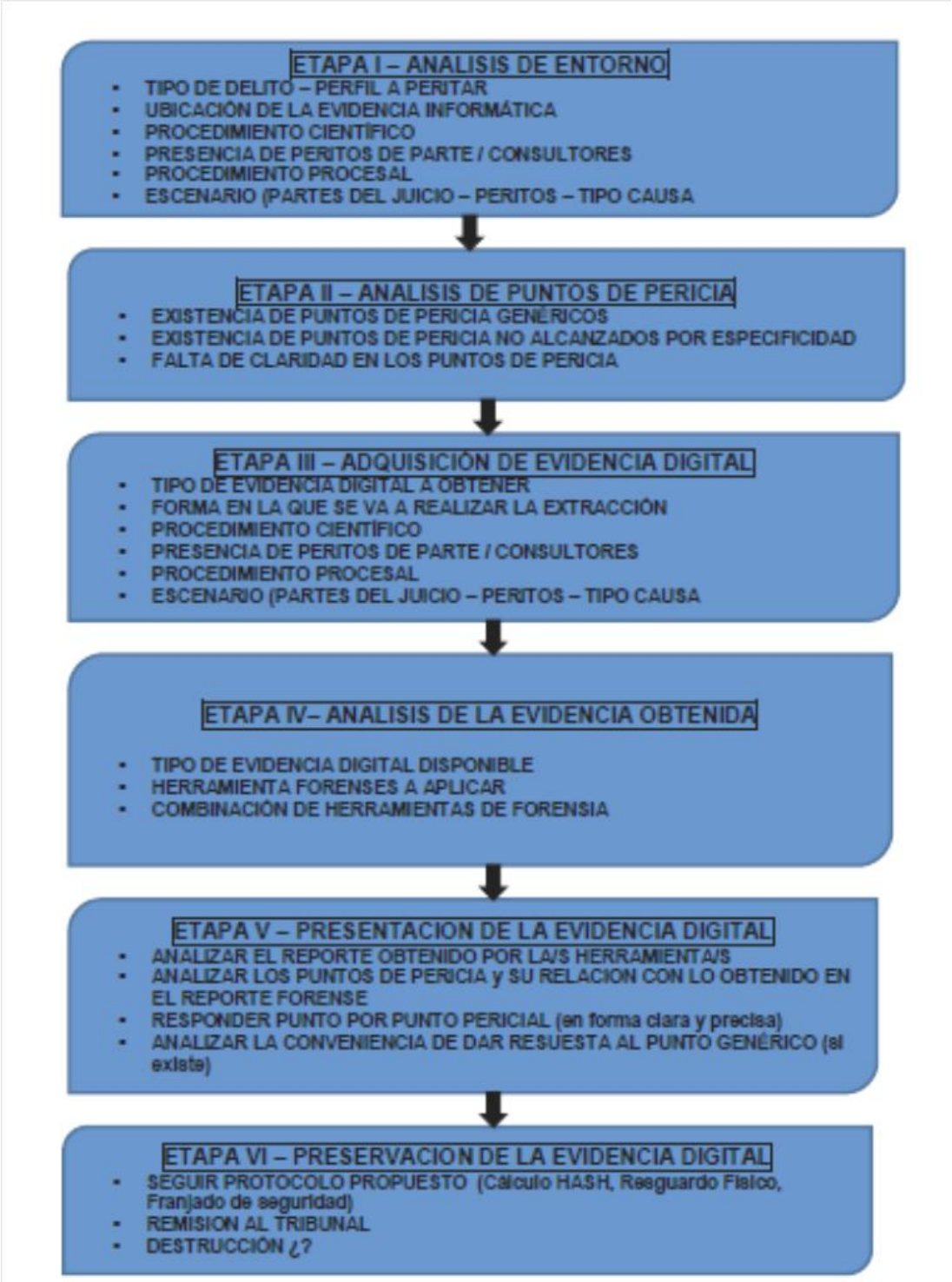

Fig. 3 Cuadro resumen de etapas para el protocolo pericial y forense. Piccirilli

Piccirilli hace especial hincapié en la cadena de custodia, la preservación de la prueba y las actividades de pericia informática, destacando el carácter volátil de la evidencia electrónica y las altas posibilidades de alteración y destrucción de la misma si no se adoptan medidas especiales para su recolección y resguardo.

Como aporte para completar el proceso de Cadena de Custodia, entendiendo como tal al proceso controlado que contiene una serie de aspectos que aseguran la trazabilidad de la prueba, presenta Formularios de Custodia Informática para el registro de datos específicos e identificatorios de cada paso de manipulación de la evidencia, pues " *es de vital importancia llevar una especie de historia clínica de todos los pasos que se siguen con la evidencia, siendo este un elemento sumamente frágil y volátil*."

Esa volatilidad es la principal diferencia con otros tipos de evidencia delictuales, por lo que es indispensable aplicar un protocolo, el cual es propuesto en la tesis de su autoría, y también contar con elementos físicos para la preservación correcta de equipos y de la misma evidencia.

En relación a la pericia informática determina que el punto de partida son los puntos de pericia, encomendados por alguna de las partes que intervienen en el conflicto legal, que es indispensable entender el perfil del problema o el delito a peritar, ya que no hay dos pericias iguales aunque se trate del mismo delito y que la pericia informática puede incluir, aunque no necesariamente, a la forensia informática.

En resumen, el análisis forense debe reconstruir el hecho, con todos los datos posibles y disponibles para presentar la cadena de acontecimientos y la secuencia temporal del ataque, incluyendo la identificación de la vía de ingreso al sistema/dispositivo vulnerado, que herramientas utilizó el atacante y además, tratar de identificar al autor sobre todo si es necesario iniciar acciones penales.

Como se expresó anteriormente, en este enfoque las investigaciones forenses digitales consideran el caso cuando se ha cometido, o se ha descubierto, el delito o incidente, cuando se ha incautado el dispositivo sospechoso y se han establecido puntos de pericia.

En este escenario se tiende a ignorar qué ha sucedido con el objeto de la investigación antes del incidente de seguridad y antes de la decisión de realizar una investigación.

Es así que puede ocurrir que la evidencia necesaria exista, que sea hallada por el investigador forense o en el peor de los casos puede suceder que no la encuentre o que

esté adulterada o incompleta, lo que posiblemente traerá aparejado que no se descubra que pasó y no se pueda acusar al delincuente informático.

Para tratar de subsanar este aspecto es necesario contar con un enfoque que pueda definir, antes de que ocurra un incidente, puntos de recolección de potencial evidencia que sustenten no solo la investigación forense sino también la continuidad digital del negocio.

En el siguiente punto se avanza y se describe este tipo de enfoque de recolección de datos digitales.

3.2.2 Enfoque preventivo-Recolección de datos a priori de un evento de seguridad. Forensic Readiness

El enfoque *Forensic Readiness* también llamado *Preparación Forense* involucra varios aspectos relativos a la seguridad, la gestión de riesgos y la protección de activos de una organización.

El término, fue enunciado por John Tan [23] quien lo describió a través de dos objetivos que apuntan a resguardar la posible evidencia antes de que ocurra el incidente. Esos objetivos son:

- maximizar la capacidad del entorno para reunir evidencia digital confiable y,
- minimizar el costo forense durante la respuesta a un incidente.

Robert Rowlingson [24] complementó estos objetivos definiendo a la *Forensic Readiness* como a la capacidad de una organización de maximizar el uso potencial de la evidencia digital a la par que minimiza el costo de una investigación, añadiendo que es la anticipación a un incidente de seguridad en comparación con la respuesta a incidentes.

Para ambos, la premisa es que los datos recolectados puedan ser utilizados no solo como insumo para el análisis de posibles incidentes de seguridad y de soporte de recuperación para la continuidad del negocio, sino también como prueba legal, lo que involucra el aseguramiento de los datos a medida que se realiza la recolección activa de los mismos.

Por ende, es vital tener la capacidad de procesar los datos con eficacia y contar con el personal capacitado que conozca la manera de garantizar que se conserve intacto el potencial de la evidencia digital.

Este enfoque plantea que estar preparado para reunir y utilizar evidencia también puede tener beneficios como elemento disuasorio considerando los altos porcentajes de infracción de políticas internas de seguridad.

Además se identifican aspectos técnicos y no técnicos, tales como time-stamping, la fortaleza de los sistemas y el compromiso del kernel, destacando seis factores básicos que afectan la preservación de la evidencia y el tiempo de investigación:

a) Como se hace el registro.
b) Quién hace el registro.
c) Qué se ha registrado.
d) Si se cuenta con un sistema de detección de intrusos (IDS).
e) Los métodos de adquisición forense que se van a utilizar
f) Los procedimientos para manipular la evidencia.

Un procedimiento preventivo para la adquisición y preservación de evidencia puede ser simple y efectivo, sin embargo, la complejidad del entorno objeto del análisis exige que la definición de los detalles de este procedimiento sean precisados desde el inicio con el fin de identificar los activos de la organización, seleccionar los datos a preservar y maximizar el uso de la posible evidencia digital.

Otro punto de relevancia es el costo monetario de un incidente, que sumará horas/días para el trabajo forense, para la restauración del sistema comprometido y para la detección de otros sistemas vulnerables.

En consideración, una adecuada planificación de respuesta a incidentes puede abordar estas cuestiones, incluyendo medidas que pueden ser incorporadas desde el momento que se diseña la red o se planifica una política de seguridad para toda la organización.

3.2.3 Modelado de la preparación forense

A medida que se considera a la preparación forense como actividad clave en las organizaciones han surgido algunos modelos que consideran diversos factores.

Pooe y Labuschagne [25] avanzan en un modelo conceptual, el cual se presenta en la Figura 4, que identifica cuatro actividades principales con categorías y sub-categorías o sub-actividades que pueden ser clasificadas en proactivas y reactivas.

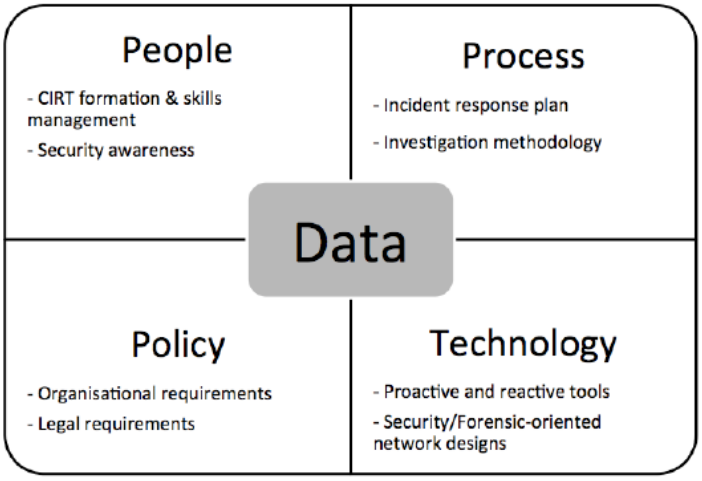

Fig.4. Modelo conceptual Digital Forensic Readiness (DFR)
Pooe y Labuschagne

a) Categoría Personas: reúne actividades relacionadas con los recursos humanos y profesionales del sector capacitados en seguridad y en comunicación organizacional. Estos últimos tienen a su cargo campañas y cursos de concientización sobre aspectos de la seguridad, la prevención y detección de incidentes. Es recomendable contar con un equipo de respuesta rápida a los incidentes representativo de todos los sectores relacionados, como por ejemplo área de sistemas, de soporte, jurídico, etc. La falta de organización, capacitación y equipamiento necesario para el equipo puede impactar negativamente en la planificación y aplicación de la preparación forense.
b) Categoría Procesos: involucra actividades y procedimientos para recolectar y asegurar la evidencia. Requiere de documentos operativos que detallen las políticas de la organización, el plan de respuesta a incidentes y la metodología de análisis forense que se utilizará. En esta categoría es un aspecto crítico recolectar la evidencia sin contaminarla y asegurar un almacenamiento que resguarde la integridad de la misma.
c) Categoría Políticas: Esta categoría refiere a las políticas organizacionales necesarias para facilitar la investigación forense, para disuadir la ocurrencia de delitos informáticos internos y las estrategias para responder a los ataques. Involucran además, las políticas de almacenamiento, planes de capacitación del personal y guías de manejo de protección de activos y evidencias. Es necesario que estas políticas sean públicas para que el personal de cada sector esté informado y comprometido en su cumplimiento.

d) Categoría Tecnología: Una organización necesita asegurar que cuenta con la tecnología necesaria para el funcionamiento de su negocio pero también para prevenir y detectar incidentes de seguridad informática. En este punto hay diversas herramientas comerciales, generalmente de un alto costo, y soluciones de código abierto que pueden integrarse a la organización para mantener un sistema activo de prevención y detección de incidentes.

Jan Collie [26] recopila y presenta otros modelos para apoyar el argumento de que dos componentes clave de la preparación forense son: una estrategia de gestión de incidentes basada en la participación de toda la compañía y un enfoque iterativo de repensar ideas estratégicas para la planificación.

- **Preparación Forense como Proceso**

Este primer modelo presenta a la preparación forense como un proceso, donde el principal objetivo es preservar y recopilar evidencia digital para que se pueda informar en una investigación, o ante el poder judicial, sobre una violación a la seguridad de los datos. El acento está en no perder o alterar inadvertidamente la evidencia digital durante la incautación de equipos en la escena de un delito.

Los cuatro objetivos identificados en este modelo y ordenados por su importancia son: identificar la evidencia, preservar la evidencia, recuperar la evidencia, presentar la evidencia.

En el siguiente grafico se muestra una representación de las etapas de este proceso:

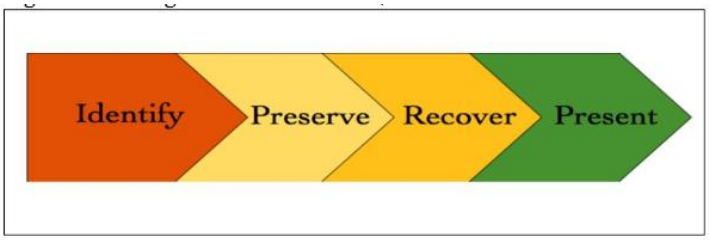

Fig.5. Digital Forensic Readiness (DFR) como proceso. Jan Collie

Las etapas descriptas en este modelo requieren de acciones que aseguren la integridad y la trazabilidad de la evidencia. También es necesario determinar los procedimientos y herramientas utilizadas para su recuperación. La etapa de presentación puede demandar formatos legales específicos si la organización tiene que presentar informes ante el poder judicial.

- **Modelo HAUS de preparación forense**

Este segundo modelo de Collie deriva del análisis de diversos artículos e investigaciones relevantes sobre el tema. Posee, según su autora, las características de Homogéneo, Responsable y de Estrategia Unificada (*Homogeneous, Answerable and Unified Strategy*- HAUS). Indica que el proceso de preparación forense es impulsado por el nivel gerencial y se entrega a todo el personal de la organización, no solo al personal técnico. Es un modelo de planificación inclusiva, basado que en cada empleado debe saber, por adelantado, que datos se necesitan proteger y que hacer, como hacerlo y quien es el responsable ante un incidente de seguridad. De esta manera se pretende involucrar a toda la organización en las etapas de un proceso proactivo, cíclico y siempre operativo.

La figura 6 muestra las fases de este modelo continuo (AAA Aware-Alert-Always-on) que serán la base del modelo HAUS. Las etapas implican:

a) Pensar lo que necesita protección

b) Planificación: cómo detectar un problema, contenerlo si es posible y quién lo necesita saber

c) Recopilación de información

d) Revisión de información

Fig.6. Modelo AAA Aware-Alert-Always-on –DFR. Jan Collie

El modelo HAUS de estrategia general (Figura 7) puede ser adaptado y utilizado por organizaciones de cualquier tamaño. Una característica clave del modelo es que cada departamento de la organización debe tener su propio ciclo del modelo AAA (Aware-Alert-Always-on), la información derivada se reporta a las personas, dentro de la cadena de mando, que pueden actuar. El input y la información de todos los departamentos deben ser agrupados y las acciones propuestas puestas a discusión por los representantes que forman el siguiente eslabón en la cadena de mando.
El input fluye en ambos sentidos, desde el personal a la gerencia y desde la gerencia al personal.

Para comenzar con la implementación de HAUS la organización debe identificar:
a) ¿Qué departamentos deberían participar?
b) ¿Quién responde en cada departamento?
c) La cadena de mando

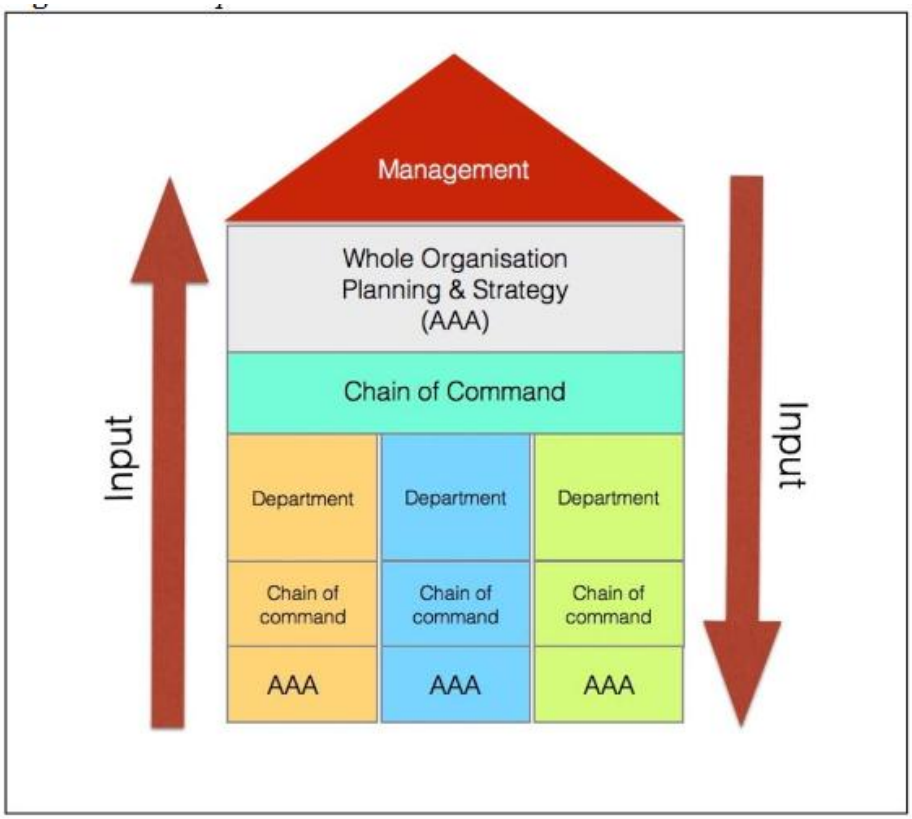

Fig.7. Modelo HAUS- DFR. Jan Collie

Si bien los modelos descriptos por Pooe, Labuschagne y Collie muestran algunas diferencias de implementación, hay una coincidencia general que apunta a resaltar la necesidad crítica de proteger los datos que pueden ser considerados evidencia y que es requisito el compromiso de toda la organización en el proceso de planificación forense que se presenta en el siguiente punto.

3.2.4 Factores en la planificación forense

Sin importar que modelo implemente la organización es necesario contar con un plan que sirva de base para evaluar el entorno, para ayudar en el diseño de un plan de acción, para acordar políticas integrales y también para construir una cultura interna de la seguridad de la información.

En ese contexto, algunas de las actividades clave en la planificación de Forensic Readiness son:

- Definir los escenarios o activos que pueden requerir de pruebas digitales;
- Identificar las fuentes disponibles y los diferentes tipos de posibles pruebas, incluyendo los procedimientos de descubrimiento de evidencia (e-discovery);
- Establecer una forma segura de obtención de pruebas para cumplir con el requisito de admisibilidad legal;
- Establecer una política para el almacenamiento seguro y para la manipulación segura de la evidencia;
- Garantizar el seguimiento para detectar y prevenir incidentes mayores, y para determinar rápidamente cual es el vector de ataque.
- Capacitar al personal de modo que todos entiendan su papel en el proceso de pruebas digitales y la sensibilidad jurídica de las mismas;
- Garantizar el control jurídico para facilitar la acción en respuesta al incidente.
- Especificar las circunstancias cuando se debe iniciar una investigación formal completa (que puede usar la evidencia digital).

El registro centralizado es una de las claves para asegurar la eficiencia de los sistemas de detección de intrusos y también para una correcta estrategia forense. Esta centralización permite, además, que herramientas específicas puedan ser aplicadas en todos los datos de registro desde múltiples plataformas. Un punto de almacenamiento centralizado para los datos de registro es más fácil de asegurar, de copiar (backup) y de adquirir para el

análisis. En este aspecto, y considerando el volumen de la posible evidencia a recolectar, será necesario pensar en soluciones e infraestructuras adecuadas y suficientes para obtener una buena perfomance.

Cuando se cuenta con un único repositorio de registros es necesario disponer de la infraestructura tecnológica adecuada para que dé soporte eficiente y también de planes de contingencia individualizados y diseñados para el repositorio.

Según lo descripto por Tan, cuando el registro se dirige desde muchos dispositivos en la red a un único repositorio, la sincronización del tiempo se convierte en un problema. Cuantos más dispositivos haya en la red, puede ser dificultoso mantenerlos todos sincronizados y sin tiempos sincronizados, registrar será confuso. La evidencia es más convincente cuando las marcas de tiempo en el recurso comprometido, el sistema de detección de intrusos y el servidor de registro centralizado son iguales, es decir registran todo lo que sucedió al mismo tiempo. Existen diversos mecanismos de sincronización para varias plataformas, por ejemplo, para redes basadas en IP, el protocolo *Network Time Protocol (NTP)* especificado en la RFC 0958 es uno de los más utilizados.

En este contexto forense es imprescindible el sellado de tiempo (*time-stamping*) lo cual puede implementarse mediante la firma digital de los registros recolectados utilizando un hash, que además de la integridad puede asegurar el no repudio y la privacidad de los registros.

La autentificación de la evidencia requiere que estos mecanismos de certificación estén acordes a las leyes de cada país y de lo que la propia organización tenga especificado en su política de seguridad.

La organización como contexto empresarial para recopilar y usar evidencia digital ha sido reconocida en una serie de documentos recientes. En coincidencia con otros autores, Yasinsac y Manzano [2002] señalan que las políticas empresariales pueden mejorar el análisis forense de computadoras y redes y proponen seis categorías de políticas para facilitar la investigación forense.

Estas categorías están diseñadas para ayudar a las organizaciones a prevenir incidentes de seguridad internos y para posicionarse de la mejor manera cuando se requiere dar respuesta a los ataques. Se focalizan en:

Retención de información: recopilación de pruebas para actuar como defensa ante demandas a la organización y como elemento de disuasión para ciberdelincuentes internos o externos.

Planificación de la respuesta: como parte de la preparación forense se pueden diseñar mecanismos de respuesta a los incidentes. Estos mecanismos deben incluirse en el plan de seguridad de la organización.
Entrenamiento: es necesario contar con un plan de entrenamiento para el personal, avalado a nivel organización y que involucre a todos los niveles de seguridad.
Acelerar la investigación: una investigación eficiente y rápida, con acciones inmediatas da como resultado una interrupción mínima del negocio.
Prevenir actividades anónimas: la Preparación Forense puede extender el objetivo de la seguridad de la información al más amplio espectro, abarcando desde delitos informáticos, protección de la propiedad intelectual, fraude o extorsión. Además de estar preparados para acciones legales puede se pueden respaldar sanciones a los empleados basadas en esa evidencia digital.
Proteger la evidencia. Un enfoque sistemático para el almacenamiento de pruebas puede reducir significativamente los costos y los tiempos de la investigación. Los datos recolectados producto de un incidente/intrusión tienen múltiples usos, pueden ser de uso interno para estudio de una vulnerabilidad o como evidencia en un proceso judicial, pero también son insumo para formular planes de respuesta a incidentes.

Los costos de implementación de la preparación forense pueden ser significativos, particularmente en organizaciones que no tengan desarrollado el proceso de gestión de la seguridad de la información. Como beneficio, que una organización tenga el control de la investigación forense y que cuente con procedimientos planificados para preservar la evidencia tiene impacto directo en el plan de respuestas a incidentes y con la continuidad del negocio.

Para ahondar en estas cuestiones, en los capítulos 5 y 6 de este trabajo se presenta a modo de guía, un modelo por etapas y un caso práctico diseñado para una organización pequeña que parte de una evaluación de riesgos de los activos y finaliza con

recomendaciones de buenas prácticas en la implementación de la Preparación Forense pensando en la continuidad digital del negocio.

Considerando los objetivos de la *Forensic Readiness*, es importante que todos los niveles, incluido la alta gerencia, acepten y participen de la planificación de la implementación.

En este sentido, las Pautas de Preparación Forense (NICS) [27] describen que el enfoque *Forensic Readiness* cuenta con un nivel apropiado de capacidad y madurez para poder preservar, recolectar, proteger y analizar evidencia digital, y con las condiciones necesarias para que esta evidencia pueda ser utilizada efectivamente en cualquier asunto legal; en investigaciones de seguridad; en procedimientos disciplinarios; en un tribunal laboral; o en una corte de justicia.

Plantea que, de hecho, el análisis forense digital no debería utilizarse exclusivamente en una actividad posterior a un incidente en la que se investigue, sino que debería planificarse cuidadosamente en la fase de preparación. De esta manera se podría optimizar considerablemente la restauración y reparación de daños ocasionados por el incidente.

Por lo tanto, es conveniente considerar a la Preparación Forense dentro de la fase de preparación del proceso de investigación digital y tratar de determinar todos los puntos que deben ser contemplados dentro de la política de la organización.

Dauda Sule, CISA [28] destaca que en caso de que el negocio de una organización quede paralizado por un evento no deseado o imprevisto, ya sea natural o provocado por el hombre, la empresa necesita recuperarse y continuar. Como resultado, las estrategias como la respuesta a incidentes, la concientización, la recuperación de desastres y la planificación de la continuidad del negocio se han convertido en componentes básicos de la estructura operativa de las organizaciones.

Además de los problemas de recuperación, un incidente no deseado también puede dar lugar a otros problemas, como reclamos de seguros, asuntos legales y cuestiones reglamentarias. En el transcurso de la recuperación e investigación, pueden surgir reclamos contra empleados, terceros o incluso la organización, por ejemplo, en relación con lo que condujo al incidente. ¿Pudo haber sido negligencia, intento malicioso, fraude o sabotaje? La evidencia digital se vuelve muy importante cuando surgen tales problemas en una organización que usa infraestructura de TI, incluso si el uso es mínimo. Los usuarios de sistemas de información dejan huellas digitales cada vez que usan los sistemas, ya sean sistemas informáticos, teléfonos inteligentes, teléfonos móviles, tablets

o redes (Internet, intranets, redes telefónicas) huellas que se pueden recuperar con la correcta aplicación de herramientas de análisis forense.

Sule amplía los objetivos originales definidos por Tan, enumerando otros que deberían incluirse en la etapa de planificación de la preparación forense. Ellos son:

- ✓ Recopilar evidencia legalmente admisible, sin interferir en los procesos de negocio.
- ✓ Recopilar evidencia sobre posibles delitos que podrían tener un impacto adverso en una organización
- ✓ Tratar de que la investigación se realice con un costo proporcional al incidente minimizando la interrupción de las operaciones.
- ✓ Minimizar la interrupción de operaciones por investigaciones.
- ✓ Garantizar que la evidencia tenga un impacto positivo en el resultado de cualquier acción legal

Por último, lo recopilado en este capítulo deja en evidencia que diferentes autores coinciden en la importancia de la preparación forense para la continuidad del negocio, como metodología preventiva para la respuesta de incidentes y en que es necesaria su planificación desde las etapas iniciales de las políticas de seguridad que implemente la organización.

Un aspecto a considerar, y que tiene relación con el tamaño de la organización, es la infraestructura de almacenamiento necesaria para dar soporte al enfoque de Preparación Forense. Se deberá calcular adecuadamente la cantidad de información a resguardar para equilibrar con una solución de almacenamiento que brinde la perfomance requerida. Este punto escapa del alcance de este trabajo de tesis, pero se incluye como tema para futuros trabajos.

CAPITULO 4. Continuidad digital para el soporte de Forensic Readiness

4.1 Introducción

The National Archives, el archivo oficial para el Gobierno del Reino Unido, departamento encargado de conservar más de 1000 años de documentos nacionales, es un organismo experto a nivel mundial en gestión de la información y resguardo de registros tanto físicos como digitales y proponen un aporte muy interesante al tema de la continuidad digital. Ofrecen una serie de guías sobre este tema que pueden aplicarse a cualquier tipo de organización y parten del conocimiento de lo que es la continuidad digital, su gestión y su relación con la preparación forense, las cuales están relacionadas con la *CESG Good Practice Guide* on *Forensic Readiness* (*Good Practice Guide No. 18*) del National Cyber Security Centre (Centro Nacional de Ciberseguridad- UK) [29] las que se toman como base para este capítulo.

4.2 Continuidad digital

La continuidad digital es entendida como la capacidad de usar la información de la organización de la manera en que se necesite y durante el tiempo que se requiera. Esto significa gestionar eficazmente la información digital a través de periodos de cambio, de modo que permanezca completa, disponible y por lo tanto utilizable según sea necesario.
La gestión de la continuidad digital puede ayudar a una organización a proporcionar la seguridad de que está gestionando eficazmente la información para satisfacer sus requisitos de preparación forense.
La **continuidad digital y la preparación forense** se apoyan mutuamente, desde el inicio de la planificación de la continuidad o de la política de seguridad convirtiéndose esta preparación en uno de los requisitos del negocio y una actividad clave en la identificación de activos de información de la organización. Si la organización pierde la continuidad

digital puede ser incapaz de encontrar, acceder y utilizar la información que precisa y tampoco podrá asegurar la integridad de su propia información.

En ocasiones es posible recuperar la información una vez que se pierde la continuidad digital, pero es un proceso costoso que consume tiempo y no asegura resultados positivos.

La guía *Managing digital continuity,* [30] describe un proceso de cuatro etapas que una organización puede seguir para administrar la continuidad digital de manera coherente y efectiva. Este modelo es flexible: se puede ingresar en cualquier etapa y ejecutar las acciones que se necesiten. También se puede ajustar el alcance para que cubra toda la organización, solo una unidad de negocios individual o si se está administrando un cambio específico.

Las etapas clave en la gestión de la continuidad digital son:

- Etapa 1. Plan de acción: donde se establecen los objetivos, personal que trabajará y aspectos de administración de la continuidad digital en toda la organización. En esta etapa es necesario considerar el alcance de su trabajo y sus prioridades. Uno de los más importantes aspectos tanto de la preparación forense como de la continuidad digital es el valor temporal de los activos digitales, que dependiendo del tipo de información puede ser de horas o de años.
- Etapa 2. Definir los requisitos de continuidad digital: esta etapa implica comprender qué tipo de información se tiene, el valor de la misma y las características del entorno técnico que la respalda, es decir identificar los activos y realizar un mapeo de estos con los requerimientos del negocio.
- Etapa 3. Evaluar y gestionar los riesgos para la continuidad digital: Comprende la definición de estructuras de gobierno TIC y de gestión de riesgos, la designación de responsabilidades y la evaluación del nivel de riesgo actual.
- Etapa 4. Mantener la continuidad digital: En esta etapa se explica el proceso continuo de integrar la continuidad digital en los procesos de la organización de manera que se mantenga la usabilidad de la información a través del tiempo y frente a los posibles cambios tecnológicos y organizacionales.

La continuidad digital es la base para la preparación forense, ya que una vez que se haya identificado qué evidencia puede ser requerida, debe considerarse cómo se va a recuperar y como se hará uso de esa información cuando sea necesario. Gestionando la continuidad digital la organización se asegura la usabilidad que necesita de su información.

La *Guía de Buenas Prácticas de la CESG sobre Preparación Forense* (Guía de Buenas Prácticas No. 18) describe doce principios importantes que las organizaciones deben observar como parte de su adopción de la preparación forense, de los cuales los principios 9 y 10 están fuertemente relacionados con la continuidad digital. Ellos son:

- **Principio 1. Contar con una política de Forensic Readiness**. Es esencial tener un enfoque documentado de la preparación forense con el fin de que pueda demostrarse su adopción formal por la organización y permitir su práctica efectiva tanto interna como externa. Este principio define diferentes niveles de capacidad que pueden ser adoptados en la política y que escalan de acuerdo a los principios definidos de gestión de riesgo y otros factores organizacionales.
- **Principio 2. Responsable.** Este principio establece que se debe designar al responsable, a nivel organización, del proceso de Forensic Readiness, puede ser el Analista de Riesgo, un profesional TI o un director, el cual debe tener la posibilidad de tomar decisiones estratégicas en la seguridad de la información.
- **Principio 3. Punto único de contacto**. Establecer un único punto de contacto, reconocido y consistente, durante la planificación y para coordinar la investigación. Este punto de contacto debe trabajar estrechamente con la organización, con el departamento legal y con otras partes interesadas en cada etapa de la investigación. Este rol de facilitador lo puede tener una persona o un grupo
- **Principio 4. Definición de Capacidad y Requisitos**. Seleccionar un objetivo de capacidad basado en la de gestión de riesgos y en respuesta a la necesidad definida. Este nivel de capacidad se puede utilizar para elegir requisitos genéricos de la política para luego adaptarlos a los locales. Este nivel de capacidad y los requisitos deben ser revisados continuamente para que coincidan con el riesgo cambiante.
- **Principio 5: Actividades de planificación basadas en escenarios**. Las organizaciones deben adoptar una metodología de planificación y preparación forense basada en escenarios para, de esa manera, aprovechar la experiencia de negocio adquirida.
- **Principio 6. Integración con gestión de incidentes y otros procesos relevantes**. Las organizaciones deben integrar los planes de preparación forense con la gestión de incidentes y otras actividades relacionadas con la planificación organizacional. Es importante que la Forensic Readiness no sea tratada como una

disciplina aislada ya que esto conduciría tanto a ineficiencias como a conflictos inevitables.

- **Principio 7: Normativa de investigación forense.** Las investigaciones deben aplicar estándares o guías de buenas prácticas para realizar las pruebas forenses y las mismas deben estar en consonancia con la normativa jurídica de cada país.
- **Principio 8: Aseguramiento de la calidad y competencia**. Cualquier capacidad forense digital interna o externa empleada por una organización debe aplicar procesos formales de garantía de calidad y competencia de todo el personal involucrado en el manejo de la evidencia durante las investigaciones.
- **Principio 9: Gestión de registros.** Las organizaciones deben mantener la calidad y eficacia de sus sistemas de gestión de registros con el fin de que se puedan tomar como en un tribunal o para atender cualquier requisito legal o regulatorio. Esto está directamente relacionado con la posibilidad de reconstrucción de la secuencia de eventos del incidente.
- **Principio 10: Acceso a la información**. Las organizaciones deben proporcionar procesos apropiados de recuperación de registros y mecanismos para que cualquier requisito de revelar información pueda ser eficiente y segura. Tales divulgaciones deben ser manejadas de acuerdo a la legislación y reglamentos pertinentes. Nota: En el caso de Argentina este principio tiene directa relación con la Ley de Protección de Datos Personales.
- **Principio 11. Lograr consenso.** Se debe procurar un enfoque abierto y colaborativo dentro de la organización, de esta manera se puede subir el nivel de aceptación a los métodos utilizados para la detección y manejo de incidentes de la seguridad de la información. Asimismo, se fortalece el compromiso institucional con el cumplimiento la política de seguridad de la organización.
- **Principio 12. Mejora continua.** Las organizaciones deben tener un proceso de revisión de la administración y de los planes de preparación forense, sobre todo a medida que estos van alcanzando grados de madurez superiores. En cada nivel de madurez, los resultados pueden parecer muy diferentes de los primeros análisis.

Es evidente que el conocimiento de una organización es mucho más que los datos, es la base de información indispensable para la toma de decisiones a niveles gerenciales y por ello es uno de sus principales activos estratégicos.

Por sus características intrínsecas la información digital es más vulnerable que la información en papel y a medida que organizaciones públicas y privadas, digitalizan todos sus procesos el aseguramiento la información es una demanda crítica de todos los niveles de la misma porque afecta directamente a la reputación e imagen de la organización.

Se mantiene como factor clave el compromiso de todas las personas de cada sector de la organización tanto para enfrentar el cambio operativo como así también en la aplicación de las políticas de seguridad. Y como esto implica una variación en la forma de utilizar la información, es recomendable realizar una evaluación de impacto sobre los activos de información con la participación de las personas relacionadas con cada activo para, de alguna manera, tratar de mitigar la resistencia al cambio que se pueda presentar. Lograr un entendimiento compartido puede ayudar tanto en el compromiso para cumplir como en la toma de decisiones estratégicas.

El tema de la continuidad digital es abordado por el mundo empresarial bajo la denominación de *Business Continuity Management (BCM*) presentando una compilación de procesos que permiten identificar y evaluar los riesgos potenciales que podrían interrumpir la actividad normal en la organización. El BCM como programa de gestión integral parte de un diagnostico de la organización para arribar a un plan de acción que minimice el impacto de los riesgos sobre el negocio tratando de garantizar la continuidad operativa. Ya sea se trate de un negocio, una organización del sector público o una organización benéfica, debe saber cómo puede continuar en cualquier circunstancia, y en algunos casos también como responder ante normas de aplicación legal o financieras vigentes en cada país.

La norma ISO 22301:2012 es la primera norma internacional para la gestión de la continuidad de negocio y se ha desarrollado para ayudar a las empresas a minimizar el riesgo del tipo de interrupciones. Especifica los requisitos necesarios para planificar, establecer, implantar, operar, monitorear, revisar, mantener y mejorar de forma continua el Sistema de Gestión para responder y recuperarse rápidamente de las interrupciones.

Para finalizar, la implementación de procesos de mejora continua es un componente ineludible para ayudar a mantener la calidad y actualización de los procedimientos que se adopten para la continuidad digital y son parte de cualquier estrategia que busque el crecimiento de una organización.

CAPITULO 5. Buenas Prácticas en la implementación de Forensic Readiness

5.1 Introducción

En los capítulos anteriores se describieron conceptos relacionados con forensia digital, con los estándares y modelos aplicables al resguardo de evidencia, con metodologías de recolección de datos, distintos modelos conceptuales de preparación forense y con la continuidad digital como meta a alcanzar por una organización.

En este capítulo se recopilaran algunos de ellos y otros aspectos para avanzar en la definición de un conjunto de buenas prácticas para la implementación de la Preparación Forense, que es el objetivo específico de este trabajo de tesis y a tal fin se propone un modelo organizado en etapas que describe las buenas prácticas y los resultados a alcanzar en cada una de ellas.

5.2 Preparación forense: Guía de buenas prácticas

No existe una normativa estandarizada para implementar la preparación forense en una organización, no obstante en lo que sí coinciden los diversos autores, normativas y estándares analizados anteriormente en este trabajo de tesis es que la protección de la información es un punto crítico al que cualquier organización debería presentar atención y preocuparse por adoptar mecanismos para asegurar tanto el resguardo de información como su propia continuidad como negocio.

Por ello a continuación se aporta una Guía de Buenas Prácticas [31] como base de partida para la implementación de Forensic Readiness, la cual está dividida en cinco etapas elementales a considerarse cuando se piensa en adoptar un enfoque preventivo. Esta estructura en etapas permite minimizar la complejidad del proceso, así la organización puede avanzar en la medida de su capacidad pero de manera constante, sabiendo que a mayor nivel de madurez alcanzará procesos y procedimientos más detallados y de mejor calidad.

En el diagrama 1 se representan las etapas propuestas, las actividades mínimas que comprenden y los resultados a lograr como producto de cada etapa

5.2.1 Etapas

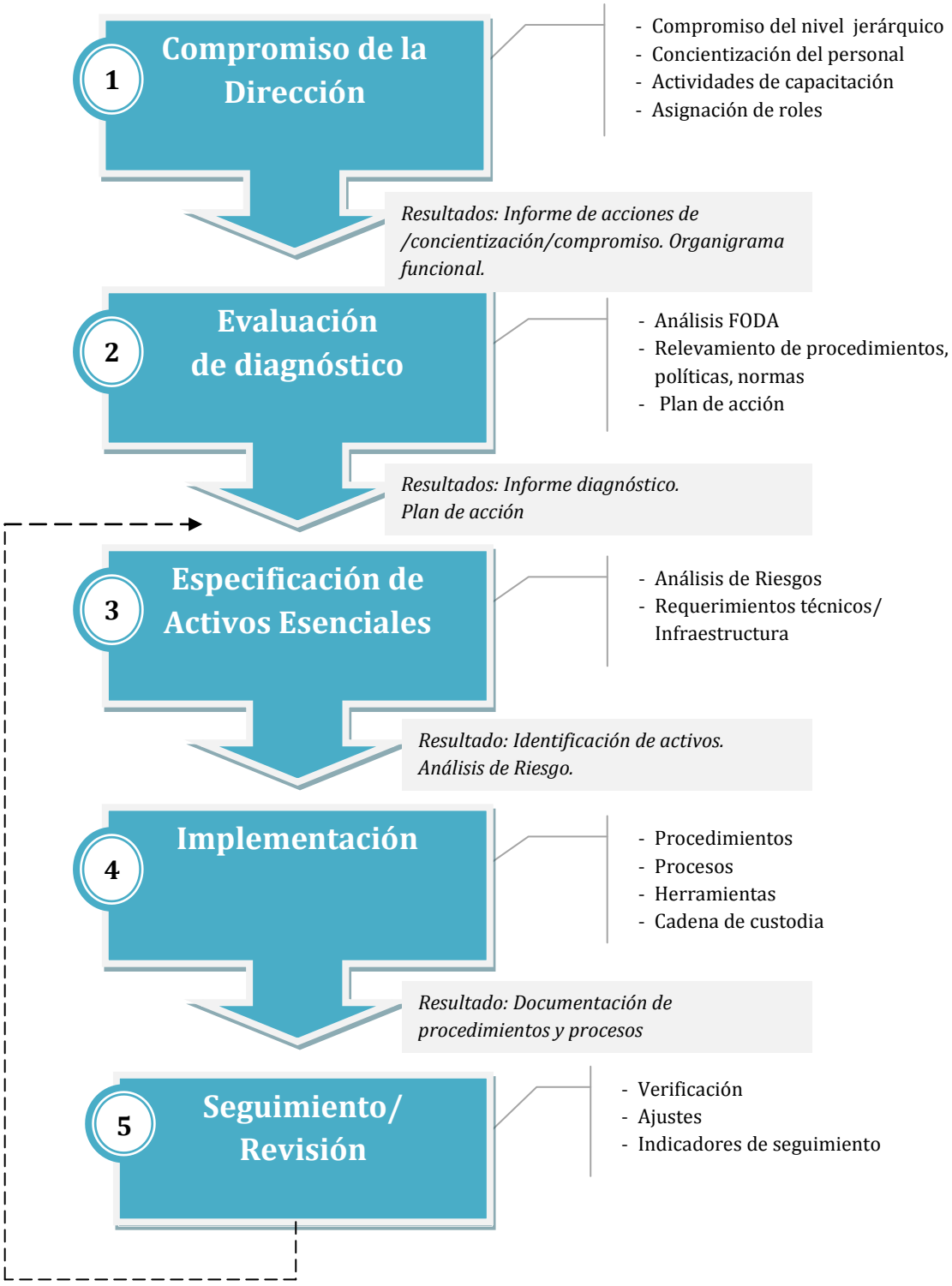

Diagrama 1. Etapas para la preparación forense

Etapa 1. Compromiso de la Dirección

Por lo general, implementar un sistema de seguridad en una organización trae aparejados diversos cambios que impactan tanto en la cultura organizacional como así también en el estilo de trabajo de cada puesto dentro de la estructura.

Cuando se piensa en implementar un enfoque Forensic Readiness, donde los controles sobre la información son muy estrictos, la dirección de la organización tiene una tarea esencial: comprometerse y tratar de lograr el compromiso de todos los niveles. Es fundamental que los niveles jerárquicos asuman la responsabilidad porque son los que tienen una visión estratégica y entienden claramente los objetivos de negocio.

Teniendo en cuenta que en la preparación forense con un solo punto en el que falle la recolección ocasionará que la trazabilidad e integridad de la evidencia se vea afectada, es de suma importancia el compromiso de todos los sectores donde se implemente este enfoque.

Según el tamaño o tipo de organización, para realizar estas actividades puede considerarse la designación de un líder o promotor del cambio, que facilite la transición hacia un nuevo modelo de trabajo.

Las reuniones informativas, capacitaciones en seguridad informática y acciones de concientización ayudaran a que cada persona esté al tanto de los procedimientos adoptados, que pueda participar en las diferentes fases de la implementación y de esta manera avanzar hacia la meta de que toda la organización preserve la seguridad de los datos.

Un rol destacado tendrán los puestos de administrador del sistema de información, el administrador de redes de datos y el administrador de la seguridad ya que sobre ellos recae la responsabilidad técnica de aplicar los procedimientos específicos sobre los datos a recolectar. Deben estar capacitados profesionalmente en seguridad informática, en ciberseguridad, en herramientas de Ethical Hacking, entre otros, para contar con las competencias y habilidades adecuadas para este proceso de preparación forense. Serán los primeros que deberán detectar las fallas de seguridad y reaccionar en consecuencia, tratando de mantener operativa la infraestructura de la organización, aplicando las herramientas de forensia adecuadas, asegurando la evidencia y dando rápida respuesta para mantener la continuidad digital.

Como resultado de esta etapa se debe producir un documento que detalle las acciones de capacitación y concientización llevadas a cabo, indicando el grado de cumplimiento y la cantidad de personal que ha participado en las diversas instancias. Contar con un

organigrama funcional, al menos con la designación de las funciones antes mencionadas y roles responsables, puede ser de gran ayuda

Etapa 2. Evaluación de diagnóstico

De acuerdo a las acciones realizadas en la Etapa 1, el personal de la organización estará en condiciones de participar de este diagnostico aportando desde las características propias de sus puestos de trabajo en relación a cuestiones de seguridad y actividades relacionadas con el tratamiento de los datos. Como herramientas participativas de diagnóstico pueden emplearse entrevistas, reuniones por sector y ampliadas, encuestas, cheklists y demás instrumentos que ayuden a lograr una evaluación integral de la organización y su contexto.

Por otra parte, se deben analizar los procedimientos y políticas existentes con respecto a la seguridad informática, como así también las normas y leyes vigentes que correspondan aplicar. Si no se cuenta con manuales de procedimiento, pueden describirse las acciones que se realizan para la gestión de incidentes de seguridad, los planes de contingencia y planes de recuperación actuales tendientes a restaurar la operatividad de los sistemas y servicios.

Asimismo es conveniente un relevamiento detallado de la infraestructura IT incluyendo dispositivos físicos, servicios, sistemas y aplicaciones, herramientas tecnológicas, estructura de almacenamiento, un mapa de la red y las conexiones, personal afectado, personal responsable de los datos, entre otros.

Como es una etapa extensa puede dividirse en sub-etapas que permitan un análisis completo e integral de todos los sectores de la organización.

El diagnóstico puede completarse con un test de intrusión y un análisis FODA para conocer las amenazas, debilidades, oportunidades y fortalezas de la organización, sobre todo en lo relativo a la seguridad interna y externa.

Es recomendable que se cuente con la participación activa de todos los sectores tanto en el relevamiento, en el análisis FODA y en la elaboración del diagnostico de situación de la organización.

Como productos de esta etapa se dispondrá de un diagnostico completo y un plan de acción que identifique los objetivos y el alcance que guiaran la implementación de la Forensic Readiness. Este plan de acción debe detallar como mínimo:

- objetivos

- el alcance
- hitos por etapas
- acciones prioritarias
- asignación de tareas
- responsables de las tareas
- tiempo previsto para cada tarea
- personal técnico disponible y requerido
- identificación del responsable de la seguridad informática
- recursos asignados

Y otros aspectos que conformen un marco para llevar adelante la implementación de manera correcta. Dependiendo del tamaño de la organización este plan de acción puede ser para un sector de la misma o para su totalidad.

Se sugiere iniciar un repositorio institucional para registrar toda la información relevada en esta etapa, así como los hallazgos, el diagnóstico, el plan de acción y demás documentación relacionada.

Etapa 3. Especificación de activos esenciales

Como se ha expresado en capítulos anteriores, los datos, la información, los procesos, los sistemas y servicios son activos fundamentales para una organización. Tienen requisitos de seguridad tales como confidencialidad, integridad y disponibilidad indispensables para mantener la continuidad del negocio, la rentabilidad, la competitividad y la reputación ante los usuarios/clientes, aspectos que son requeridos en el logro de los objetivos propios de la organización.

Hay varias metodologías que sirven de base para la identificación de activos y el análisis de riesgo. En el capítulo 6 se presenta un ejemplo realizado con la metodología Magerit, adaptable a cualquier tamaño de organización y de libre utilización, la cual sirve para especificar el alcance del análisis, identificar los Activos, las Amenazas y las Salvaguardas como parte de ese análisis de riesgo. Magerit, o cualquier otra metodología de análisis que se elija, ayudará a identificar los activos y especialmente los Activos Esenciales que marcaran los requisitos de seguridad para los demás componentes del sistema.

El análisis inicia con un inventario de activos, información que puede tomarse de la etapa anterior de diagnóstico, lo cual servirá para diferenciar entre activos estratégicos, tácticos y operacionales. Los activos estratégicos son los servicios o productos que sustentan la capacidad competitiva de la organización, los activos tácticos los procesos involucrados

para la correcta entrega de esos servicios o productos, y los activos operacionales aquellas actividades que se determinan como críticas en cada proceso.

El inventario también puede emplearse para conocer el estado de situación de infraestructura y las posibles adecuaciones con vista a la implementación de la Preparación Forense, sobre todo la infraestructura de almacenamiento requerida para dar soporte a la metodología preventiva.

De ser necesario se puede ajustar el plan de acción luego de seleccionados los activos esenciales, con indicación de prioridades, datos a recolectar, tiempo de recolección y responsable asignado.

Es imprescindible comprender la operatoria, protocolos asociados, la estructura y demás características del activo seleccionado, porque ese conocimiento ayudará a detectar rápidamente un comportamiento sospechoso o anómalo. Además se puede recurrir a publicaciones especificas que mantienen actualizadas las vulnerabilidades que afectan a los sistemas, tales como OWASP y OWASP Top 10 [32] que describen los diez riesgos de seguridad más importantes de software y en aplicaciones web.

Como resultado de esta etapa se contará con un conocimiento detallado de los activos y de los riesgos asociados a los mismos, la probabilidad de ocurrencia, el impacto y los controles que se deberán efectuar para su mitigación.

Cada uno de los riesgos identificados deberá estar relacionado con una o más de las dimensiones de seguridad informática establecidas como requisitos del sistema, lo cual permitirá establecer adecuadamente el nivel de riesgo y los controles específicos que correspondan.

Etapa 4. Implementación

Definidos los activos esenciales y efectuado el análisis de riesgo correspondiente, se puede iniciar con la etapa de implementación de Forensic Readiness.

Esta es una instancia más bien técnica donde, sobre los activos identificados se iniciará la recolección de datos y el tratamiento de los mismos como evidencia digital.

Los procedimientos que se apliquen sobre los datos recolectados deben orientarse a resguardar la integridad de la evidencia y a asegurar la confiabilidad y la disponibilidad como requisitos a cumplir por parte del sistema de seguridad que comienza a funcionar.

Se reitera la importancia de mantener la cadena de custodia desde el inicio, para asegurar la plena admisibilidad como prueba legal de la evidencia recolectada. Esta cadena de custodia implica el registro detallado de cada paso dado con respecto a los datos, es decir,

asegurar la trazabilidad de la información y mantener la integridad de los archivos con algoritmos de hash, como por ejemplo MD5, SHA1 o SHA-256 que producirán una huella digital unívoca para el conjunto de datos.

Por idénticos motivos, deben documentarse las herramientas tecnológicas utilizadas tanto para recolectar como las aplicadas en el análisis de datos, las responsabilidades asignadas y las prioridades consideradas con respecto al resguardo de datos.

El valor temporal que la organización le otorgue a sus datos determinará las necesidades de infraestructura de almacenamiento para el registro centralizado de los datos considerados evidencia. Este repositorio deberá recibir tratamiento con el rango de Activo esencial.

La aplicación de herramientas de forensia informática se realiza en esta etapa tanto para la vigilancia de incidentes como para el análisis de datos. Existen numerosas soluciones comerciales y open source que deberán ser cuidadosamente seleccionadas dependiendo de sus prestaciones, utilizando también una combinación de varias herramientas diferentes para lograr una mayor potencia y perfomance.

El enfoque de Ethical Hacking dará el marco adecuado para aplicar herramientas de testeo para realizar pruebas y así lograr un profundo conocimiento del sistema, de las redes, de aplicaciones y dispositivos para detectar fallos con fines defensivos y de mitigación de incidentes, todo esto bajo un estricto código de conducta profesional. Metodologías tales como OSSTMM [33] del ISECOM pueden considerarse como marco de trabajo para realizar testing, análisis y mediciones de seguridad para establecer las mejores estrategias de defensa.

Las vulnerabilidades descubiertas deben ser reportadas al responsable designado de manera inmediata para su tratamiento, como así también deberá hacerlo cualquier persona de la organización que crea estar frente a un fallo de seguridad.

Como resultado de esta etapa se obtendrán procedimientos y procedimientos detallados de la implementación de Forensic Readiness, incluyendo descripción de herramientas empleadas, formularios que registren cada paso de la cadena de custodia e instrumentos de reporte de incidentes.

Etapa 5. Seguimiento/Revisión

Se requiere un seguimiento activo de todo el proceso de la Preparación Forense tanto para verificar su correcto funcionamiento como así también para detectar a tiempo errores o falencias que puedan ocurrir.

Es relevante evaluar si las actividades desarrolladas se realizan conforme a lo previsto y la confidencialidad, integridad y disponibilidad de los datos se encuentra garantizada.

Para esta evaluación se pueden construir indicadores de seguimiento que reflejen los resultados de eficiencia y efectividad de lo implementado y que ayuden a tomar decisiones al respecto, entre otros:

- resultados de auditorías;
- resultados de análisis de intrusión;
- observaciones recibidas;
- información de avance sobre acciones preventivas y correctivas;
- mediciones y actualizaciones de vulnerabilidades.

Los cambios en la organización, en la tecnología y en las leyes aplicables en cada país pueden producir modificaciones en los objetivos de negocio, en las amenazas detectadas, en las oportunidades del entorno y en la efectividad de los controles implementados por lo que es conveniente la revisión periódica de los activos esenciales y los riesgos que los afectan.

Obviamente esta revisión puede dar lugar a ajustes sobre las etapas propuestas en este modelo, pero es importante que desde la Dirección se mantenga una actitud proactiva de vigilancia sobre el desarrollo de todas las actividades relacionadas, para asegurar los recursos requeridos y como mejora continua del proceso de Forensic Readiness.

En el capitulo siguiente se presenta un caso de aplicación de implementación de Preparación Forense en una pequeña organización ficticia, aplicando lo descripto en las etapas 3, 4 y 5.

Capitulo 6. Presentación de un caso de utilización de buenas prácticas en entornos Forensic Readiness

6.1 Introducción

En este capítulo se presenta la aplicación de las etapas 3, 4 y 5 propuestas en el modelo de buenas prácticas en un entorno de una pequeña organización que cuenta con un servidor web como principal activo para sus actividades. Por este motivo, se comienza con un estudio exploratorio del protocolo HTTP, luego se realiza la identificación de activos asociados a este protocolos y un análisis de riesgo y además la identificación de los puntos de control seleccionados para la recolección de datos.

Las pruebas fueron realizadas en una red de trabajo LAN Ethernet con sistema operativo y herramientas de forensia open source. Para la recolección de datos se simuló un ataque de Denegación de Servicios sobre el servidor que también se uso como insumo para análisis de weblogs.

6.2 Protocolo HTTP

Hypertext Transfer Protocol (HTTP) es un protocolo de nivel de aplicación del modelo TCP/IP que presenta características que lo hacen factible de ser utilizado en sistemas abiertos, heterogéneos, distribuidos, colaborativos e hipermediales [34]. Se caracteriza por ser un protocolo cliente- servidor que define la estructura de los mensajes de requerimiento/respuesta así como también la forma en que se realiza el intercambio de dichos mensajes entre los clientes y los servidores web.

Como parte del proceso de desarrollo de HTTP en el año 1996 el HTTP Working Group (HTTP-WG) del Internet Engineering Task Force (IETF) publicó la RFC 1945, que describe el “uso común” de HTTP/1.0 pero sin intentar crear un estándar formal mas allá de las diversas implementaciones existentes. En 1999 el HTTP-WG desarrolló un protocolo mejorado, conocido como HTTP/1.1, cuya especificación está descripta en la RFC 2616 [35].

Si bien desde sus inicios se ha considerado como un protocolo simple, HTTP se ha convertido en la base sobre la que corren otros protocolos e infraestructuras de aplicaciones.

Las características principales del protocolo incluyen:

- Intercambio de mensajes de solicitud-respuesta en formato ASCII.
- Uso de los servicios del protocolo TCP.
- Soporte de transferencia de objetos multimediales, enviando los datos binarios codificados en cadenas de caracteres (Tipos MIME).
- Ocho operaciones (métodos) que permiten llevar a cabo una transacción entre el cliente y el servidor: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS, CONNECT.
- Cada operación HTTP requiere una conexión con el servidor que es liberada al término de la misma. HTTP/1.1 mejora este procedimiento implementando el mecanismo “HTPP Keep Alive”.
- No mantiene estados. Los servidores tratan cada petición como una operación independiente.
- Utiliza URL's para identificar recursos.
- Se presentan algunos problemas de seguridad debido al intercambio de mensajes en texto plano.

Tanto HTTP/1.0 como HTTP/1.1 utilizan los servicios del protocolo TCP, puerto 80, como mecanismo de transporte fiable de transferencia de datos, de manera que los mensajes intercambiados entre el cliente y el servidor web son recibidos en orden y sin modificaciones.

HTTP es definido como un protocolo sin estado debido a que los servidores web no almacenan información sobre los clientes. Los servidores web tratan cada requerimiento en forma independiente de cualquier otro lo que implica que cada requerimiento deba incluir tanta información como el servidor necesite para satisfacerlo.

Como consecuencia de lo anterior, cuando un cliente pide por distintos recursos de un mismo servidor (por ejemplo las imágenes de una página web), entonces habrá una gran cantidad de requerimientos que serán casi idénticos, tornando repetitivo al protocolo. Una forma de mejorar la eficiencia en este sentido es mediante la compresión de las cabeceras [36].

Por otra parte, dado que algunas aplicaciones web requieren mantener un registro sobre la actividad del usuario (por ejemplo las aplicaciones de carritos de compra) se introdujo

el concepto de cookies para almacenar información de estado. Las cookies fueron presentados por Netsacape en la versión 1.1 de su browser y luego estandarizadas por el IETF en la RFC 2109.

El protocolo HTTP puede utilizar tanto conexiones no persistentes como persistentes. En una conexión no persistente solo se puede transferir un único objeto web sobre una conexión TCP en cambio las conexiones persistentes permiten transferir múltiples objetos web durante el transcurso de una única conexión. HTTP/1.0 utiliza conexiones no persistentes, mientras que HTTP/1.1 emplea por defecto conexiones persistentes. No obstante, los clientes y servidores web HTTP 1.1 pueden ser configurados para utilizar conexiones no persistentes [37].

Como ya se ha mencionado, el protocolo se basa en operaciones de solicitud-respuesta, basadas en mensajes en formato ASCII. El cliente establece una conexión con el servidor y envía un mensaje con los datos de la solicitud. El servidor procesa el requerimiento y responde con otro mensaje similar, conteniendo el estado de la operación y su resultado. Las operaciones pueden adjuntar un objeto o recurso sobre el que actúan, y cada objeto web es identificado por su URL.

El formato de los mensajes HTTP es el siguiente:

Mensaje de requerimiento
GET /dir/page.html HTTP/1.1 Host: www.facultad.edu User-agent: Mozilla/ 4.0 Connection: close Accept -language: sp *(línea en blanco)*

Mensaje de respuesta
HTTP/1.1 200 OK Connection close Date: Wed, 12 jun 2019 12:00:15 GMT Server: Apache / Content-Length: 6850 Content – Type: text/html *(datos)*

- La primera línea del mensaje de requerimiento es la operación que se solicita al servidor, mientras que en el mensaje de respuesta indica el resultado especificado por un código numérico.

- Las cabeceras son un conjunto de headers que condicionan el funcionamiento del protocolo.
- Una línea en blanco indica el final de los encabezados.
- Por último, el cuerpo del mensaje con información opcional (por ejemplo, el documento HTML que devuelve el servidor).

Si bien el protocolo HTTP ha servido con éxito a la Web durante muchos años, algunas de sus características afectan negativamente el rendimiento de las aplicaciones. Por ejemplo, los clientes que necesitan realizar varios requerimientos suelen utilizar múltiples conexiones al servidor para reducir la latencia. Sin embargo, establecer demasiadas conexiones conduce a problemas de congestión que afectan la perfomance de la red y de las aplicaciones, así como a un uso excesivo de recursos por parte de los clientes y al intercambio de información redundante en las cabeceras de los mensajes.

Las limitaciones anteriores dieron lugar a una revisión del protocolo HTTP y al desarrollo de una nueva versión: HTTP/2 definido en la RFC 7540 [38]. Esta versión permite la entrega de múltiples mensajes de requerimiento/respuesta sobre la misma conexión, utiliza una codificación más eficiente para los campos de los encabezados HTTP y posibilita asignar prioridades a los requerimientos.

El protocolo resultante tiende a ser más amigable para la red en la medida que se utilizan menos conexiones TCP (en comparación con HTTP/1.x), logrando un mejor uso de la capacidad disponible.

El protocolo HTTP2 fue pensado para ser la próxima generación de protocolos para las aplicaciones web. Puede ser dividido lógicamente en tres capas:

- La capa de transmisión, que incluye los flujos, las tramas y el control de flujo;
- HPACK, que define la codificación binaria y el protocolo de compresión; y
- la capa semántica, que es una versión mejorada de HTTP/1.1 enriquecida con capacidades de tipo “server Push”.

Entre las características más relevantes del protocolo HTTP/2 pueden mencionarse:

- **Binario**. Es un protocolo binario lo cual le otorga independencia de cualquier código.
- **Tramas**. Usa formato de mensajes basados en tramas. Las tramas son la unidad de datos básica de HTTP2, que reemplazan los mensajes con formato cabecera-

cuerpo de HTTP/1.1. Hay tramas de encabezados, tramas de información, tramas de configuración que comparten el mismo formato.

- **Multiplexación**. El protocolo es completamente multiplexado. Cada trama enviada sobre una conexión HTTP2 está vinculada a un "flujo". Un flujo es una asociación lógica que identifica una secuencia independiente y bi-direccional de tramas intercambiadas entre un cliente y un servidor sobre una conexión HTTP2. Los destinatarios procesan las tramas de un flujo en el orden en que son recibidas. La multiplexación de flujos permite que las tramas de diferentes flujos sean mezcladas sobre una misma conexión. Es decir, dos o más secuencias individuales de datos se combinan en una sola en un extremo y luego vuelven a separarse en el otro extremo.

- **Prioridad**. Cada flujo tiene una prioridad que indica su importancia y que puede ser cambiada dinámicamente en tiempo de ejecución.

- **Compresión**. Utiliza compresión de encabezados para reducir el consumo de ancho de banda producido por requerimientos similares de un mismo cliente, introduciendo para tal fin el formato de compresión HPACK e incluye soporte para tramas DATA comprimidas con gzi.

- **Ventana deslizante**. Control de flujo mediante ventana para cada flujo individual

- **Petición de envío desde el servidor**. Implementación de un mecanismo de "server push", que permite que los servidores envíen proactivamente a la cache del cliente las respuestas que estos puedan llegar a necesitar.

HTTP/2 incorpora el uso obligatorio de TLS (Transport Layer Security) para una comunicación segura, conservando la misma semántica y la compatibilidad con las versiones 1.0 y 1.1 El protocolo se implementa si el cliente y el servidor tienen soporte y en el caso de que alguno de los dos no lo tengan, en la negociación de protocolo, se acuerda usar las versiones anteriores. Actualmente la mayoría de los browsers y entornos de servidor cuentan con implementaciones oficiales para la nueva versión

El uso de un esquema de codificación binario y del mecanismo de compresión HPACK tiene por objetivo reducir el ancho de banda necesario, mientras que los demás componentes del protocolo están pensados para reducir los retardos de ida y vuelta en la red y para acelerar los tiempos de carga de páginas web complejas [39]

A partir de estas características, el protocolo HTTP/2 intenta conducir hacia una Web más rápida, eficiente y segura.

6.3 Seguridad en HTTP

El protocolo HTTP es considerado un protocolo no seguro debido a que la información viaja a través de la red en texto plano. Por ende, los diseñadores de HTTP/2 realizaron un esfuerzo significativo en identificar y manejar los riesgos a la seguridad del nuevo protocolo, tanto a partir de decisiones de diseño como de guías de implementación. Sin embargo, algunas implementaciones de servidores HTTP/2 pueden no seguir completamente estas guías, tornándose vulnerables a distintos tipos de ataques.
En consecuencia, algunos posibles ataques identificados sobre servidores HTTP/2 incluyen los que se describen brevemente a continuación ([1]):

- **Stream reuse:** El mecanismo de multiplexación de flujos permite que múltiples sesiones compartan una misma conexión HTTP/2. El riesgo en este caso surge a partir de que la partición de la conexión es puramente lógica y, en consecuencia, puede ser utilizada para manipular el servidor o para enviar tramas fuera de contexto. Un flujo HTTP/2 representa un único ciclo de requerimiento-respuesta y una vez cerrado el identificador del flujo no debería ser usado sobre la misma conexión. El ataque de reutilización de flujo utiliza el identificador de un flujo ya cerrado sobre la misma conexión para enviar un nuevo requerimiento. Cuando el servidor recibe dos requerimientos con el mismo identificador, entonces puede resultar en comportamientos no esperados.
- **Slow read:** El mecanismo de control de flujo de ventana de HTTP/2 se asemeja al de TCP, el cual ha sido blanco de distintos ataques. Un atacante puede configurar el tamaño de la ventana de entrada a un valor muy pequeño mientras requiere un recurso de gran tamaño del servidor, pudiendo mantener así la conexión abierta por un largo, o incluso ilimitado, período de tiempo, consumiendo recursos del servidor. Al repetir varias veces esta operación, el cliente malicioso puede provocar una denegación de servicios en el destino. Este ataque resulta más simple de implementar en HTTP/2 gracias a las capacidades de multiplexación del protocolo que permiten que el atacante envíe un gran número de flujos sobre una

[1] Imperva. Hacker Intelligence Initiative.

misma conexión TCP. Aún cuando el servidor mantiene también una única conexión de nivel de transporte, dedica un hilo de procesamiento por cada flujo, y por consiguiente el resultado es que se consuman todos los hilos de trabajo. La asimetría entre los recursos requeridos por el cliente y los dedicados por el servidor, hacen que un atacante puede dirigir este tipo de ataques a servidores de gran capacidad aún con mínimos recursos computacionales.

- **Dependency Cycle DoS**: Los mecanismos de prioridades y dependencias de HTTP/2 son opcionales. El tamaño del árbol de dependencias no está limitado, por lo que un servidor que confíe en un cliente puede ser inducido a construir un árbol de dependencias que consumirá toda su memoria. Al mismo tiempo, la generación de ciclos de dependencias o cambios rápidos en las dependencias, pueden resultar en consecuencias inesperadas, tales como grandes consumos de CPU o de memoria. Estas características pueden ser explotadas para producir ciclos de dependencias que generen loops infinitos o saturación de memoria, y que afecten el rendimiento del servidor.
- **HPACK Bomb:** La idea detrás de este ataque es enviar una cantidad relativamente pequeña de datos, que luego de descomprimirse consumen una cantidad significativa de memoria en el destino. Al repetirse la acción, el servidor puede consumir toda su memoria imposibilitando el acceso de otros clientes. La RFC de HTTP/2 no establece restricciones en cuanto al tamaño de cabeceras individuales, lo cual hace que el mecanismo de compresión HPACK sea vulnerable a este tipo de ataques de denegación de servicios.

A modo resumen, el siguiente cuadro compara algunos puntos destacados sobre las principales características de las tres versiones HTTP [40]:

Versión	HTTP/1.0 (1996)	HTTP/1.1 (2000)	HTTP/2 (2015)
RFC	*RFC 1945*	*RFC 2616*	*RFC 7540*
Manejo de requerimientos	Un requerimiento entregado por vez sobre una conexión.	Mecanismo HTPP Keep Alive: varios requerimientos pueden utilizar múltiples conexiones con el servidor para reducir la latencia.	Múltiples mensajes de requerimiento/ respuesta sobre una misma conexión. Permite asignar prioridades a los requerimientos.
Header	Formato texto	Formato texto	Formato binario. - Compresión de header (Algoritmo HPACK).
Multiplexación	No permite conexiones simultáneas	No permite conexiones simultáneas	Permite múltiples solicitudes y respuestas en paralelo usando la misma conexión TCP, enviando cada requerimiento en un stream diferente.
Servidor	Descarga de recursos a solicitud del cliente (primero HTML, luego CSS, JS, imágenes, enlaces)	Descarga de recursos a solicitud del cliente (primero HTML, luego CSS, JS, imágenes, enlaces)	Tecnología server push: Permite cargar los archivos (CSS, JS, imágenes) desde el servidor al cliente sin que éste lo pida.

Cuadro 1. Comparativa versiones protocolo HTTP

6.4 Identificación de Activos. Análisis De Riesgo

Para este trabajo de tesis se consideró un caso hipotético de una pequeña organización que se dedica a proveer servicios web y con esa base se seleccionó al servidor web como el activo estratégico más relevante para dicha organización.

Se realizó un análisis de riesgo sobre los sistemas TIC relacionados con la página web de la empresa para identificar, analizar y cuantificar las vulnerabilidades, conocer la probabilidad de pérdida de la información y determinar las posibles acciones preventivas y correctivas que podrían llevarse a cabo.

Para este análisis de riesgo y para realizar el inventario, se utilizó como base la metodología Magerit 3.0, metodología de análisis y gestión de riesgos de libre utilización propuesta por el Consejo Superior de Administración Electrónica de España, que brinda un método sistemático para analizar riesgos, un catálogo de elementos y una guía de técnicas para el tratamiento de los mismos.

Esta metodología, adaptable a cualquier tamaño de organización, considera para el análisis de riesgos los siguientes elementos:

a) **Activos**: son los elementos del sistema de información (o estrechamente relacionados con este) que soportan la misión de la Organización
b) **Amenazas:** sucesos que pueden afectar a los activos causando un perjuicio a la Organización
c) **Salvaguardas:** (o contra medidas), son medidas de protección desplegadas para que aquellas amenazas no causen [tanto] daño.

Con estos elementos se puede estimar:

1. El **impacto**: lo que podría pasar
2. El **riesgo**: lo que probablemente pase

El análisis de riesgos permite analizar estos elementos de forma metódica para llegar a conclusiones con fundamento y proceder a la fase de tratamiento. Informalmente, se puede decir que la gestión de la seguridad de un sistema de información es la gestión de sus riesgos y que el análisis permite racionalizar dicha gestión.

La metodología ayuda a clasificar los activos en:

- **Activos esenciales**: información que maneja y servicios que presta el sistema de información, lo cual marca los requisitos de seguridad para todos los demás componentes del sistema

- **Arquitectura del sistema:** Se trata de elementos que permiten estructurar el sistema, definiendo su arquitectura interna y sus relaciones con el exterior- Comprende a los datos, claves criptográficas, servicios, software, equipamiento informático, redes de comunicaciones, soporte de información, equipamiento auxiliar, instalaciones, personal

En caso de que se requiera se puede utilizar el documento OWASP TOP 10 para identificar los riesgos y vulnerabilidades específicas del servidor web, tanto desde el punto de vista técnico como del organizacional, para poder así hacer un diagnóstico más completo de los riesgos.

6.4.1 Alcance del análisis de riesgo

El alcance del análisis de riesgo para el sistema web, y para el protocolo presentado en este trabajo, abarca desde que se registra un acceso al servidor en un log hasta el almacenamiento y protección de los datos que se recolectarán como evidencia de la transacción.

Preponderantemente se tratará de mantener la integridad y la disponibilidad de los archivos logs, con especial indicación de detección de comportamientos anómalos a modo preventivo y, para cada uno de los requisitos de seguridad, con respecto a:

- **Integridad**: que entes no autorizados no puedan alterar, corromper o insertar datos en el log.
- **Disponibilidad**: que entes no autorizados no puedan borrar archivos logs.

Como requisitos de seguridad complementarios se deberá asegurar la trazabilidad y autenticidad de los weblogs para conocer donde se generan, quien tiene acceso y si se producen cambios se registren los mismos.

El cumplimiento de estos requisitos exigidos permitirá que los datos puedan ser utilizados como evidencia en un proceso judicial en caso de ser necesario.

6.4.2 Especificación de activos y análisis de riesgo

Tabla 1

Identificación de activo esencial

Nombre	Descripción
Activo esencial Id: **[esencial]**	[info] información [dv] datos/registros vitales de la organización [log] logs del servidor web [service] servicio web

Tabla 2

Detalle de activos

Nombre	Id	Descripción
Datos/ información	[D]	Archivos de datos, weblogs, passwords, datos de configuración
Software / Aplicaciones	[SW]	Aplicaciones web, punto de acceso al servicio, sistema operativo, sistema de backup
Hardware / equipos	[HW]	Servidor, router, firewalls, equipos de trabajo
Medios	[Media]	Dispositivos de backup
Redes de comunicación	[COM]	Red Ethernet, enlace ADSL
Personal / RR.HH.	[P]	Usuarios, personal de IT.

Dimensiones de seguridad de los activos bajo amenaza (las cuales serán marcadas con una X en las tablas siguientes)**:**

[D]- Disponibilidad

[I]- Integridad de los datos.

[C]- Confidencialidad de la información.

[A]- Autenticidad.

[T]- Trazabilidad.

Tablas de valoración de los activos y relación con dimensiones de seguridad

Tabla 3

Activo datos/información

Activo [D]	**Dimensiones de seguridad.**				
	[D]	**[I]**	**[C]**	**[A]**	**[T]**
Archivos de datos.		**[x]**		**[x]**	**[x]**
Weblogs	**[x]**	**[x]**			**[x]**
Passwords		**[x]**	**[x]**	**[x]**	
Datos de configuración	**[x]**	**[x]**	**[x]**		**[x]**

Tabla 4

Activo Software/Aplicaciones

Activo [SW]	**Dimensiones de seguridad.**				
	[D]	**[I]**	**[C]**	**[A]**	**[T]**
Aplicaciones web	**[x]**	**[x]**	**[x]**	**[x]**	
Punto de acceso al servicio	**[x]**			**[x]**	
Sistemas operativos	**[x]**	**[x]**	**[x]**		
Sistema de backup	**[x]**	**[x]**			**[x]**

Tabla 5

Activo Hardware/Equipos

Activo [HW]	**Dimensiones de seguridad.**				
	[D]	**[I]**	**[C]**	**[A]**	**[T]**
Servidor	**[x]**			**[x]**	
Routers/Firewalls	**[x]**			**[x]**	
Equipos de trabajo	**[x]**		**[x]**		

Tabla 6

Activo Medios de almacenamiento

Activo [Media]	Dimensiones de seguridad.				
	[D]	[I]	[C]	[A]	[T]
Dispositivos de backup	[x]	[x]			[x]

Tabla 7

Activo Redes de Comunicación

Activo [COM]	Dimensiones de seguridad.				
	[D]	[I]	[C]	[A]	[T]
Red Ethernet (interna)	[x]		[x]		
Enlace ADSL	[x]				

Tabla 8

Activo Personal / RR.HH.

Activo [P]	Dimensiones de seguridad.				
	[D]	[I]	[C]	[A]	[T]
Usuarios			[x]	[x]	
Personal IT			[x]	[x]	

6.4.3 Amenazas

Se presenta a continuación, de manera no exhaustiva, un catálogo de posibles amenazas sobre los activos de la organización con foco en el activo principal que es el servidor web. Para cada amenaza, identificada según la clasificación de la tabla, se tipifica el tipo de error, el activo, las dimensiones de seguridad afectadas y una descripción complementaria de la amenaza.

Amenazas y dimensiones afectadas

Tabla 9

Clasificación de las amenazas

Identificador	Tipo
N	Desastres naturales/accidentales
E	Errores y fallos
T	Del Entorno
A	Ataques a la seguridad

Tabla 10

Amenazas y dimensiones afectadas

[N.1] Fuego.	**Dimensiones.**
Tipos de activos: [HW]: Hardware [Media]: Medios Origen: **N-** Desastres naturales/accidentales	**1. Disponibilidad.**
Descripción: incendios o sobrecalentamiento que pueden afectar los recursos del sistema y su localización	
[E.1] Errores de usuario	**Dimensiones.**
Tipos de activos: [D]: Datos/Información [SW]: Software/Aplicaciones [HW]: Hardware [COM]: Redes de Comunicación [Media]: Medios Origen: **E-** Errores y fallos	**1. Integridad de los datos.** **2. Confidencialidad de la información.** **3. Disponibilidad.** **4. Autenticidad.**
Descripción: errores de uso por parte de las personas cuando utilizan los datos, servicios, redes, aplicaciones del sistema	

[E.2] Errores de administrador	**Dimensiones.**
Tipos de activos: [D]: Datos/Información [SW]: Software/Aplicaciones [HW]: Hardware [COM]: Redes de Comunicación [Media]: Medios Origen: **E-** Errores y fallos	**1. Integridad de los datos.** **2. Confidencialidad de la información.** **3. Disponibilidad.** **4. Autenticidad.**
Descripción: errores de uso por parte de las personas encargadas de administrar y supervisar el sistema.	
[E.3] Errores de configuración	**Dimensiones.**
Tipos de activos: [D]: Datos/Información [SW]: Software/Aplicaciones [HW]: Hardware Origen: **E-** Errores y fallos **A-** Ataques a la seguridad	**1. Integridad de los datos.** **2. Disponibilidad** **3. Autenticidad.** **4. Trazabilidad.**
Descripción: error en la configuración de los datos, del hardware y software producto de la acción u omisión del administrador.	
[E.4] Errores de monitorización (log)	**Dimensiones.**
Tipos de activos: [D]: Datos/Información [D.log] registros de actividad Origen: **E-** Errores y fallos **A-** Ataques a la seguridad	**1. Confidencialidad de la información.** **2. Trazabilidad.**
Descripción: inadecuado registro de actividades, registros incompletos, registros no resguardados adecuadamente, registros destruidos.	
[E.5] Alteración respaldo información	**Dimensiones.**
Tipos de activos: [D]: Datos/Información [D.log] registros de actividad [Media]: Medios Origen: **E-** Errores y fallos **A-** Ataques a la seguridad	**1. Integridad de los datos** **2. Disponibilidad** **3. Trazabilidad** **4. Confidencialidad de la información.**
Descripción: alteración del resguardo de logs, de manera accidental o premeditada. Se incluye el backup de estos datos esenciales	

[E.6] Difusión de software dañino	**Dimensiones.**
Tipos de activos: [D]: Datos/Información [SW]: Software/Aplicaciones [HW]: Hardware. [COM]: Redes de Comunicación [Media]: Medios Origen: **E-** Errores y fallos **A-** Ataques a la seguridad **T**- del Entorno	**1. Disponibilidad.** **2. Integridad de los datos.** **3. Confidencialidad de la información.**
Descripción: difusión ya sea intencional o no de virus, troyanos, ransomware, malware en el sistema.	
[E.7] Vulnerabilidades del software	**Dimensiones.**
Tipos de activos: [SW]: Software/Aplicaciones [D]: Datos/Información Origen: **E-** Errores y fallos **A-** Ataques a la seguridad	**1. Integridad de los datos.** **2. Confidencialidad de la información** **3. Disponibilidad.**
Descripción: fallas en el código que provocan errores de software, en los datos de usuario y puede dejar puertas abiertas al sistema lo que pone en juego su integridad.	
[T.1] Degradación de los soportes de almacenamiento de la información.	**Dimensiones.**
Tipos de activos: [HW]: Hardware. [Media]: Medios Origen: **T-** del Entorno	**1. Disponibilidad.** **2. Integridad.**
Descripción: se debe al paso del tiempo o a una mala preservación de los dispositivos de almacenamiento.	

[T.2] Fallo del servicio de comunicaciones.	**Dimensiones.**
Tipos de activos: [COM]: Redes de Comunicación Origen: **E-** Errores y fallos **A-** Ataques a la seguridad **T**- del Entorno	**1. Disponibilidad.**
Descripción: Cese de la capacidad para la transmisión de datos, sea por falla humana, destrucción física de los enlaces o por ataque a la seguridad	
[A.1] Suplantación de la identidad del usuario.	**Dimensiones.**
Tipos de activos: [SW]: Software/Aplicaciones [HW]: Hardware Origen: **A**- Ataques a la seguridad	**1. Autenticidad.** **2. Confidencialidad de la información.** **3. Integridad.**
Descripción: personas externas o internas a la organización que acceden a un servicio o estación de trabajo como usuario autorizado para operar	
[A.2] Manipulación de los registros de actividad (logs)	**Dimensiones.**
Tipos de activos: [D]: Datos/Información [D.log] registros de actividad Origen: **A**- Ataques a la seguridad	**1. Integridad** **2. Trazabilidad** **3. Confidencialidad de la información.**
Descripción: alteración premeditada de registros de actividad	
[A.3] Denegación de servicios.	**Dimensiones.**
Tipos de activos: [SW]: Software/Aplicaciones [D]: Datos/Información Origen: **A-** Ataques a la seguridad	**1. Disponibilidad.**
Descripción: indisponibilidad de recursos del sistema por ataques activos de denegación de servicios (DoS)	

[A.4] Destrucción de información	Dimensiones.
Tipos de activos: [D]: Datos/Información [SW]: Software/Aplicaciones [Media]: Medios Origen: **A-** Ataques a la seguridad	1. **Disponibilidad**
Descripción: eliminación intencional de la información.	
[A.5] Fallas en la seguridad interna	**Dimensiones.**
Tipos de activos: [D]: Datos/Información [SW]: Software/Aplicaciones [HW]: Hardware. [COM]: Redes de Comunicación [Media]: Medios [P]: Personal TI Origen: **A-** Ataques a la seguridad	1. **Disponibilidad.** 2. **Integridad** 3. **Confidencialidad de la información**
Descripción: eliminación/modificación intencional de la información por acción de ataques internos a la organización.	

6.4.4 Salvaguardas

Las salvaguardas permiten hacer frente a las amenazas. Debido a su carácter dinámico por aparición de nuevas tecnologías, cambio de activos, evolución de los ataques y otras cuestiones similares, Magerit no las incluye dentro del paquete solo enumera algunas como guía a considerar.

A modo de ejemplo, para este análisis de riesgo se pueden determinar salvaguardas, relacionadas con las dimensiones de seguridad, del estilo:

a.- Protecciones generales

H. Protecciones generales

H.**A** Identificación y autenticación de administrador de sistema
H. **A.C.** Control de acceso lógico
H.tools.IDS Implementación de herramientas de detección de intrusos
H.tools.CC Herramientas de chequeo de configuración
H.tools.L Herramienta de análisis de logs

b.- Protección de los datos/información

D. Protección de la información

D.A Implementación de copias de seguridad

D.C Implementación de cifrado

c.- Protección de los servicios

S. Protección de los servicios

S.**A.D** Aseguramiento de la disponibilidad

S.www protección de servicios y aplicaciones web

S.dns protección del servidor de nombres de dominio

S.http Implementación de protocolo seguro

d.- Salvaguardas relativas al personal

PS Gestión de personal

PS **A.C**. Formación y concientización

e.- Continuidad de las operaciones

BC. C Continuidad del negocio

BC. FR Implementación de Forensic Readiness

BC. PR Implementación de planes de reacción frente a desastres

Tabla 11

Cuantificación del impacto de las amenazas sobre los activos

Valor		Criterio
MA	**muy alto**	daño muy grave a la organización
A	**alto**	daño grave a la organización
M	**medio**	daño importante a la organización
B	**bajo**	daño menor a la organización
MB	**muy bajo**	irrelevante a efectos prácticos.

Tabla 12

Riesgos, probabilidad de ocurrencia, medición del impacto y dimensión de seguridad amenazada.

A. Dimensiones de valoración

[D]	Disponibilidad
[I]	Integridad
[C]	Confidencialidad
[A]	Autenticidad
[T]	Trazabilidad

B. Descripción de amenazas

[N]	Desastres naturales/accidentales
[T]	Del Entorno
[E]	Errores y fallos
[A]	Ataques a la seguridad

N°	**Riesgo**	**Probabilidad**			**Impacto**			**Dimensión Amenazada**
		Bajo	**Medio**	**Alto**	**Leve**	**Moderado**	**Catastrófico**	
R1	[N.1] Fuego	X					X	[D]
R2	[E.1] Errores de usuario		X			X		[I] [C] [D] [A]
R3	[E.2] Errores de administrador		X			X		[I] [C] [D] [A]
R4	[E.3] Errores de configuración		X			X		[I] [D] [A] [T]
R5	[E.4] Errores de monitorización (log)		X				X	[C] [T]
R6	[E.5] Alteración respaldo información		X				X	[I] [D] [T] [C]
R7	[E.6] Difusión de software dañino		X			X		[D] [I] [C]
R8	[E.7] Vulnerabilidades de software		X			X		[I] [C] [D]
R9	[T.1] Degradación soporte almacenamiento	X					X	[D] [I]
R10	[T.2] Fallo del servicio comunicaciones	X				X		[D]
R11	[A.1] Suplantación identidad de usuario	X				X		[A] [C] [I]
R12	[A.2] Manipulación registros logs		X				X	[I] [T] [C]
R13	[A.3] Denegación de servicios		X				X	[D]

R14	[A.4] Destrucción de información		X				X	[D] [I]
R15	[A.5] Fallas en seguridad interna		X				X	[D] [I] [C]

Riesgo		Probabilidad		
		Baja	Media	Alta
Impacto	Catastrófico	R1, R9	R5,R6, R12, R13, R14, R15	
	Moderado	R10, R11	R2,R3,R4, R7, R8,	
	Leve			

Escalas	Riesgo bajo	Riesgo Apreciable	Riesgo importante	Riesgo crítico

6.5 Puntos de control HTTP

Luego de este análisis de riesgo, se identificaron los puntos de control para el protocolo HTTP funcionando, para realizar esta tesis, en un entorno de trabajo LAN Ethernet compuesto por un servidor con Sistema Operativo Ubuntu Server y un Servidor Web Apache Server completándose con tres estaciones de trabajo. A todos los equipos se les asignó una dirección IP dentro del dominio de prueba *comyredes.edu*, mientras que al servidor se le asignó una dirección IP pública.

Por otra parte, se utilizó una notebook, fuera de la red Ethernet, con el toolkit *Kali Linux* versión 64bit [41] que es un sistema de código abierto basado en Debian GNU/Linux diseñado principalmente para la auditoría y seguridad informática y que cuenta con diversas aplicaciones y utilidades relacionadas.

Para este punto se consideraron trabajos preliminares sobre análisis de herramientas de software libre aplicadas a la recolección de datos [42], que se incluyen como referencia.

Como se ha descripto en capítulos anteriores, para el enfoque de preparación forense, donde cada dato debe ser tratado como evidencia digital, el resguardo de los registros de actividad para su posterior análisis es uno de los puntos críticos a considerar, con especial atención al almacenamiento, al aseguramiento de la integridad y a la trazabilidad de los mismos.

Para este trabajo se seleccionaron los siguientes datos y registros a recolectar:

- **puertos 80 y 443**: que registra el tráfico entrante y saliente del protocolo HTTP y asociados como SSL - Secure Sockets Layer.
- **archivos log** del sistema operativo Ubuntu Linux (/var/log/)
    - ***messages.log***: registro de mensajes generales del sistema. Almacena logs que llegan con prioridad *info* (información), *noticie* (notificación) o *warn* (aviso).
        - ***auth.log***: registro de autenticación. En este log se registran los *login* del sistema y los intentos fallidos se registran en líneas con información del tipo *invalid password* o *authentication failure*
        - ***btmp:*** lista de accesos fallidos al sistema.
    - ***secure***: registro de autenticación. Archivo de log para los mensajes de seguridad
    - ***utmp:*** lista los usuarios que están actualmente dentro del sistema.
    - ***wtmp:*** registra quienes estuvieron en el sistema y cuando.
- **httpd**: archivos log de Apache: *error.log* y *access.log*. El primero proporciona información de diagnóstico y registra cualquier error que ocurre en el procesamiento de los requerimientos; mientras que el segundo almacena todos los requerimientos procesados por el servidor.
- **archivos de configuración** del servidor Apache: a fin de determinar modificaciones no autorizadas en la configuración del servidor que puedan alterar su funcionamiento.

6.6 Enfoque preventivo. Recolección y resguardo de evidencia

De manera activa se realizó el monitoreo de logs y recopilación de datos según los puntos de chequeo establecidos:

- puertos 80 y 443
- archivos log del sistema operativo
- httpd: archivos log y de configuración de Apache

La especificación del período de recolección de datos dependerá de los requerimientos de la organización y de los activos que desee proteger con este enfoque. En este caso, se realizó un respaldo diario de los datos recolectados que luego fueron almacenados en medios externos (una notebook y un pendrive) con protección de integridad mediante hash. Se aclara que por ser un entorno académico de prueba, el volumen de *logs* fue manejable. Para un entorno organizacional se debería calcular un estimado semanal del volumen promedio en

bytes y de allí considerar que infraestructura de almacenamiento será la más adecuada para su implementación.

La secuencia del procedimiento para la copia diaria es la siguiente [43]:

Fig. 8 Procedimiento backup FR

Sobre la imagen ISO de los datos se genera un hash que tiene como funciones principales la autenticación del archivo y la preservación/verificación de la integridad de los datos que son considerados evidencia digital. Este hash de la copia forense permitirá verificar si la misma fue alterada con posterioridad a su obtención y mantendrá la Cadena de Custodia sobre la evidencia.

MD5 y SHA1 son dos de los algoritmos de hash más comúnmente utilizados en forensia informática, MD5 produce un valor hash de 128 bits, mientras que SHA1 produce un valor hash de 160 bits. Se pueden usar versiones más largas de SHA también; estos serán referidos por la longitud de bits del valor hash que producen (por ejemplo, SHA256 y SHA512).

El hash se generó de manera sencilla empleando el comando *sha1sum* del sistema operativo Ubuntu, que añade la suma de comprobación SHA-1 del archivo.

En la siguiente captura de pantalla se muestra el hash generado para el backup de los logs almacenados en el pendrive de respaldo.

Fig. 9 Hash generado para el backup FR

También existe la posibilidad de generar dos hashes para cada archivo, uno con SHA1 como en este caso y otro con MD5, de esta manera se aumenta se duplica el control de autenticidad e integridad de los datos.

Si se desea un mayor control de la trazabilidad de los archivos almacenados puede implementarse un control de versiones, por ejemplo con el software open source

Apache Subversion[2], que registra los cambios realizados sobre un archivo o conjunto de archivos a lo largo del tiempo.

Es conveniente llevar un control de registro de cada archivo almacenado que reúna todos los datos relacionados, tales como fecha de captura, hora, si es original o copia, el personal que realizó la copia, el hash generado y el detalle del procedimiento y herramientas utilizadas para el respaldo, independientemente de que esto se realice con *Subversion*, con cualquier otra aplicación de versionado o que se utilice una simple planilla. El punto esencial es asegurar la cadena de custodia de manera complementaria al hash que protege los datos.

Otro aspecto a considerar, y teniendo en cuenta el análisis de riesgo efectuado en el punto anterior, es el cuidado de los medios externos de almacenamiento, cualquiera sea este, que si se pierde, destruye o degrada las pruebas quedarán inutilizables.

6.7 Simulación de ataque de Denegación de Servicios (DoS)

Empleando herramientas de hacking se realizó la simulación de un ataque de Denegación de Servicios Distribuido (DDoS) a los fines de observar el comportamiento del servidor, el volumen de datos resguardados en logs y para analizar la perfomance de las metodologías en instancias de recuperación del servicio y resguardo de la evidencia.

El ataque de Denegación de Servicios (*DoS- Denial of Services*) [44], tiene como principal objetivo atacar redes y recursos de comunicaciones causando que los servicios sean total o parcialmente inaccesibles para los usuarios autorizados. Dicho ataque normalmente ocasiona la pérdida total de conectividad a la red, por la saturación intencional de los puertos con un flujo constante de información sobrecargando los recursos de los servidores y la capacidad de responder a las peticiones realizadas por los usuarios originales.

Cuando un sitio web sufre un ataque DoS los usuarios pueden notar que el sitio deja de mostrar contenido pero para la organización puede significar que sus sistemas, o activo principal en este caso, han dejado de operar. El ataque puede durar unas horas o días, puede dirigirse a un sistema o sitio o a más de uno a la vez y puede originarse en un solo punto de ataque (DoS) o desde varios puntos o vectores de ataque transformándose en

[2] Apache Subversion https://subversion.apache.org/

distribuido (DDoS), esta última variante es una de las formas más comunes de ataque a sitios web.

Los eventos DoS a menudo son provocados por la sobrecarga de los sistemas subyacentes de un servicio que se ven saturados cuando demasiados usuarios solicitan el mismo, por ejemplo un sitio web de compra en evento CyberMonday o venta de entradas para un concierto.

El problema surge cuando este DoS es malicioso y se convierte en un ataque activo a la seguridad, donde el atacante de manera premeditada intenta agotar los recursos del sitio web dejando sin acceso a los usuarios. Por añadidura, si este ataque de denegación malicioso es del tipo distribuido, DDoS, serán miles de usuarios o equipos que generarán solicitudes de servicio para sobrecargar el objetivo y esta misma característica distribuida aumenta la posibilidad de no poder localizar a los atacantes.

Para organizar el ataque, se pueden usar equipos infectados con virus o malware o redes botnet que están conformadas por un grupo de PC/dispositivos infectados y controlados por un atacante de forma remota.

El objetivo del ataque puede ser la saturación de servicios, como ser un servicio web que se ejecuta en la capa de aplicación, o directamente la destrucción del sistema o el hardware/firmware del mismo.

Para una organización es muy difícil evitar este tipo de ataques que ni siquiera se pueden mitigar en su totalidad, lo que sí debe hacer es prepararse para cuando suceda conociendo sus propios activos, el caudal de trabajo que soportan sin problemas, y teniendo un plan de contingencia que dé respuesta a este y otras modalidades de ataques a la seguridad.

Para este proyecto se simuló un ataque DoS con metodología de inundación que consiste en enviar un gran número de paquetes hacia el servidor web que en este caso era el activo identificado. Para darle la característica de distribuido, se emplearon varias maquinas virtuales actuando en paralelo, tipo *Botnet*, desde un servidor y a través de la aplicación *Hping3* para simular un ataque *SYN Flood Attack* que tenía por objetivo el servidor de la red de pruebas. La aplicación *Hping3* [3], que es una de las herramientas que integran Kali Linux, genera paquetes de petición de conexión TCP a muy alta velocidad y en modo inundación por lo que el servidor web deja su operatoria normal para responder los paquetes.

[3] HPING 3https://kali-linux.net/article/hping3/

También se empleó, desde el exterior de la red, la herramienta *Slowloris*[4] para saturar de peticiones al servidor Apache, aumentar la consumición del servicio y completar la simulación.

Como se expresó anteriormente, en casos reales, una vez detectado el ataque de DoS se debe tratar de mitigar lo más posible desplegando una serie de medidas que reduzcan el daño causado y que restauren los servicios del sistema comprometido a la normalidad. Para este proyecto se priorizó la recolección de datos para analizar el comportamiento de los logs del servidor, cuestión que se analiza a continuación.

6.8 Análisis de weblogs

Cada interacción o transacción que atiende un webserver queda registrada en un archivo *log*, mediante el cual es posible determinar, entre otros, que objetos fueron requeridos, que tipo de cliente web realizó la petición, que contenidos se visitaron, es decir, construir una instantánea de cada sesión establecida con el servidor web.

Un log contiene datos que permiten registrar la actividad de un usuario en un servidor web, tales como:

- Dirección IP del usuario
- Tiempo de acceso
- Método solicitado (GET o POST)
- URL de la página
- Protocolo (http/versión)
- Código retornado (control de éxito u error de la transacción)
- Número de bytes transmitidos

Cada uno de estos archivos se considerará como una fuente semiestructurada a no-estructurada, donde el esquema de los datos está implícito y contenido en los propios datos que se describen a sí mismo.

Los datos disponibles en los archivos logs pueden transformarse en información de interés empleando para su análisis técnicas y métodos, como por ejemplo de Data Mining [45].

En este entorno, y de manera general, lo que se conoce como Minería Web tratará de descubrir información o conocimiento así como patrones interesantes en el contenido, en la estructura y en la utilización de sitios web, diferenciándose en las siguientes aéreas:

[4] Slowloris https://github.com/gkbrk/slowloris

- Minería Web de Contenido,
- Minería Web de Estructura, y
- Minería Web de de Uso.

Específicamente, la Minería Web de uso tiene como principal objetivo extraer conocimiento útil analizando fuentes de información, tales como la almacenada en archivos log de los servidores web, por ejemplo para obtener patrones de preferencias o de perfiles de los usuarios partiendo de los datos de navegación o tráfico en la Web.

Por defecto, los servidores Web Apache utilizan el formato de log *NCSA Common Log Format* [46] para registrar las solicitudes de clientes y errores. Este formato registra la URL completa de cada recurso al que se accede. De esta forma, el log no solo es un registro bitácora de las operaciones sino también que permite realizar un análisis forense buscando actividades sospechosas.

Cada línea guardada en un archivo NCSA Common Log Format posee la siguiente sintaxis:

```
host ident authuser date request statuscode bytes
```

Ejemplo:

```
200.63.1.67 - usuario [03/Mar/2019 9:11:10:55 +0000] "GET /index.html HTTP/1.1" 200 431
```

El análisis de logs debido a su semi estructuración puede volverse complejo y tedioso, pero se pueden utilizar filtros y buscar patrones de ataque desde la línea de comandos de manera manual o, utilizar herramientas específicas de análisis, open source y comerciales, como por ejemplo LogAnalyzer, GNOME System Log, Splunk, Logstash, WebLog Expert entre otras.

Para las diversas pruebas que se realicen no deben utilizarse los archivos recolectados y resguardados como evidencia.

Por ejemplo, en el siguiente gráfico realizado utilizando la herramienta LogAnalyzer[5], se puede apreciar que el día que se realizó la simulación del ataque el log *message.log* tuvo un crecimiento abrupto para registrar las novedades del servidor, siendo un indicio de la capacidad de almacenamiento que puede requerir la preparación forense.

[5] LogAnalyzer https://www.loganalyzer.net/

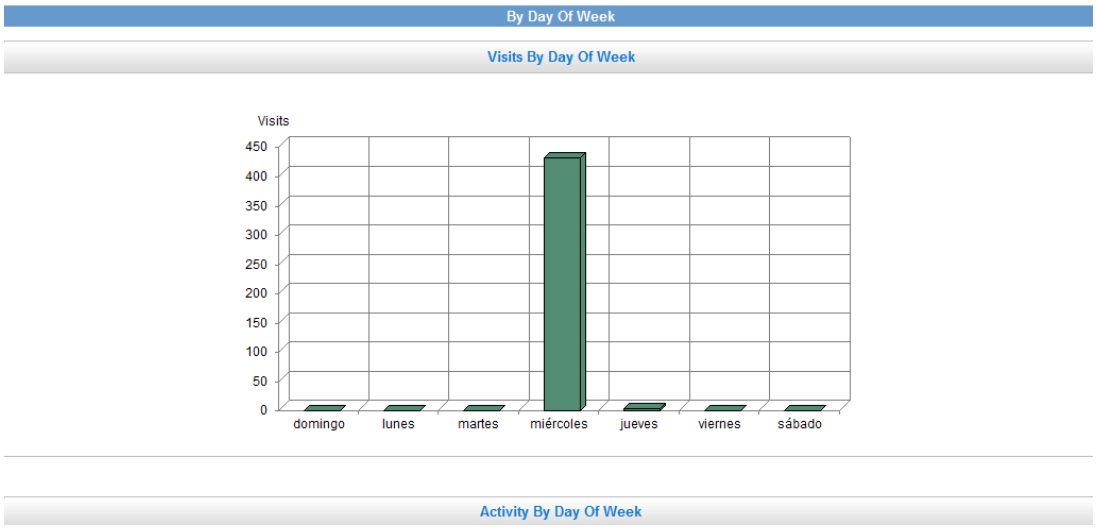

Fig.10 Visualización crecimiento log

Ese mismo día se registró un repunte de actividad anormal con detección de intentos de acceso al sistema mediante un ataque de fuerza bruta del tipo Diccionario, un método empleado para romper la seguridad de los sistemas basados en contraseñas en la que el atacante intenta dar con la clave adecuada probando todas (o casi todas) las palabras posibles de un diccionario, en este caso se utilizó uno en idioma portugués.

Esta actividad en cierta manera colaboró con la simulación del ataque DDoS realizado en este trabajo.

By Visits

Top Visits

	Visitor	Country/Region	Visits	% of Total Visits	Bandwidth
1	181.94.55.154 net.ar	Argentina	425	97,93%	0 Bytes
2	110.44.126.237 ceapred.org.np	Nepal	1	0,23%	2,85 KB
3	141.212.122.16 umich.edu	United States	1	0,23%	3,39 KB
4	123.207.99.178	China	1	0,23%	1,36 KB
5	37.146.181.196 corbina.ru	Russian Federation	1	0,23%	10,00 KB
6	60.191.38.77	China	1	0,23%	11,36 KB
7	137.226.113.11 rz.rwth-aachen.de	Germany	1	0,23%	16,88 KB
8	220.181.159.73 chinatelecom.com.cn	China	1	0,23%	11,30 KB
9	155.94.89.82 wyeth.com	United States	1	0,23%	11,32 KB
10	200.185.214.70	Brazil	1	0,23%	11,30 KB
	Subtotal		**434**	**100,00%**	**79,76 KB**
	Total		**434**	**100,00%**	**79,76 KB**

Fig.11 Análisis de log- accesos por IP

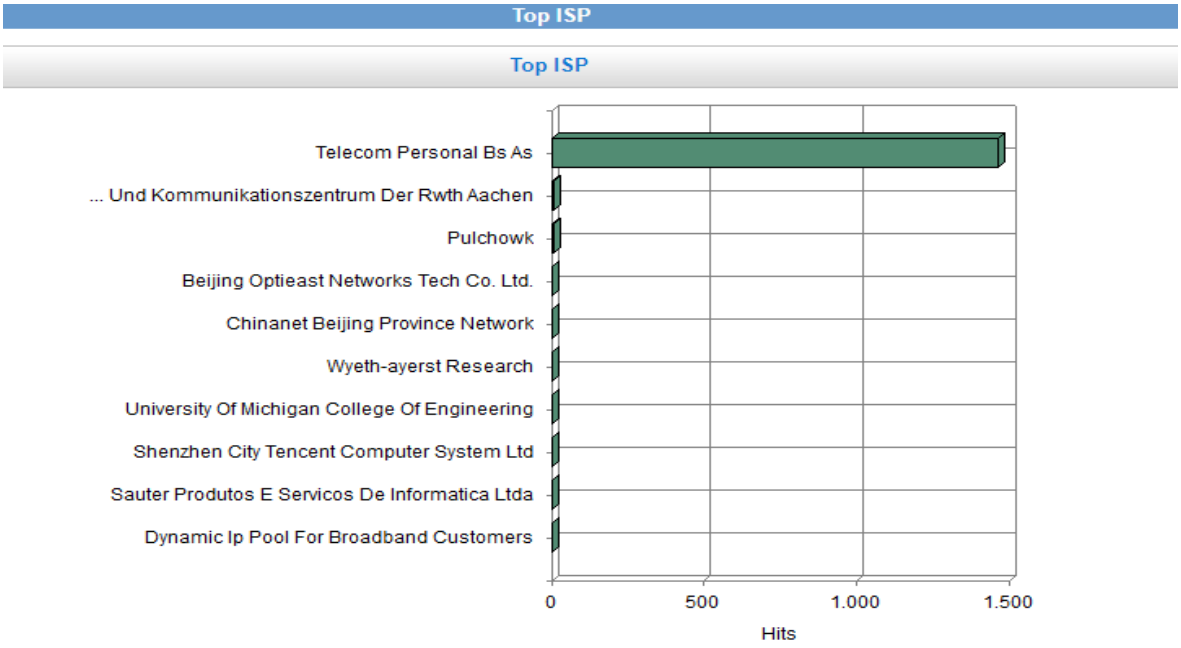

Fig.12 Accesos registrados por ISP

Nota: Telecom Personal es el proveedor utilizado para la red usada en este trabajo.

Analizando el archivo syslog con el entorno Sumo Logic [6], rastreando la dirección IP podemos ver la actividad de esos accesos sospechosos

1,482 181.94.55.154 - - [16/Aug/2017:08:40:10 -0300] "GET /?87548759470609 HTTP/1.1" 400 0 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50313; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; MSOffice 12)"
Host: 201.219.170.74 Name: access.log.13.gz Category: uploads/apache/access

1,483 137.226.113.11 - - [16/Aug/2017:07:28:28 -0300] "GET / HTTP/1.1" 200 1920 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.86 Safari/537.36 Scanning for research (researchscan.comsys.rwth-aachen.de)"
Host: 201.219.170.74 Name: access.log.13.gz Category: uploads/apache/access

1,484 137.226.113.11 - - [16/Aug/2017:07:28:28 -0300] "GET / HTTP/1.1" 200 1920 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.86 Safari/537.36 Scanning for research (researchscan.comsys.rwth-aachen.de)"
Host: 201.219.170.74 Name: access.log.13.gz Category: uploads/apache/access

1,485 137.226.113.11 - - [16/Aug/2017:07:28:28 -0300] "GET / HTTP/1.1" 200 3840 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.86 Safari/537.36 Scanning for research (researchscan.comsys.rwth-aachen.de)"
Host: 201.219.170.74 Name: access.log.13.gz Category: uploads/apache/access

1,486 137.226.113.11 - - [16/Aug/2017:07:28:28 -0300] "GET / HTTP/1.1" 200 3840 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.86 Safari/537.36 Scanning for research (researchscan.comsys.rwth-aachen.de)"
Host: 201.219.170.74 Name: access.log.13.gz Category: uploads/apache/access

1,487 137.226.113.11 - - [16/Aug/2017:07:28:28 -0300] "GET / HTTP/1.1" 200 1920 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.86 Safari/537.36 Scanning for research (researchscan.comsys.rwth-aachen.de)"
Host: 201.219.170.74 Name: access.log.13.gz Category: uploads/apache/access

1,488 137.226.113.11 - - [16/Aug/2017:07:28:28 -0300] "GET / HTTP/1.1" 200 3840 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.86 Safari/537.36 Scanning for research (researchscan.comsys.rwth-aachen.de)"
Host: 201.219.170.74 Name: access.log.13.gz Category: uploads/apache/access

Fig.13 Análisis de logs-IP

[6] SUMO LOGIC https://www.sumologic.com/

Fig.14 Análisis de logs

En esta última captura se registra la actividad de *ZmEu*, que es un escáner de vulnerabilidades que busca servidores web abiertos para atacar a través del programa *phpMyAdmin*.

Syslog tiene la particularidad de tener un formato único de datos lo que facilita el análisis de los datos de registro. Por ese motivo algunos autores recomiendan explotar esta funcionalidad y considerar que todos los dispositivos tengan la capacidad de soportar syslog, además de contemplar el uso de un servidor seguro de syslog para centralizar el registro y punto de forensia.

Para finalizar con este punto, se menciona que el ataque sobre el servidor duró aproximadamente 16 horas donde el normal funcionamiento del mismo se vio degradado en un 70%.

Aplicar una metodología Forensic Readiness ayuda a que este porcentaje de degradación y pérdida operativa no sea crítico en la recuperación de la evidencia digital y que la restauración de la operatoria normal luego del ataque sea más efectiva al contar con procedimientos de respuesta y políticas de contingencia.

Generalmente un enfoque reactivo no puede asegurar que evidencia digital no se haya contaminado durante el ataque y la recuperación de la operatividad será un proceso lento y costoso que no siempre tiene un buen final. Para la organización esto significará no solo la pérdida de operatividad temporal sino también afectará su reputación ante los usuarios o clientes, factor de gravedad añadida en un mercado dinámico y globalizado.

Conclusiones

Diariamente millones de dispositivos, redes, sistemas y organizaciones se enfrentan a incidentes de seguridad que pueden poner en jaque sus funcionalidades. Este contexto complejo y cambiante obliga a las organizaciones a pensar en una política de seguridad de la información con mecanismos y estrategias de prevención de incidentes que proporcionen una arquitectura de seguridad correctamente definida para ofrecer un plan y un conjunto de políticas que describan tanto los servicios de seguridad ofrecidos a los usuarios como los componentes del sistema requeridos para implementarlos.

A la par, es un requerimiento cada vez más determinante contar con personal calificado en áreas de seguridad y ciberseguridad y con un modelo de seguridad integrado a los demás procesos de la organización que le dé la capacidad de enfrentar los riesgos y retos tecnológicos actuales.

En este trabajo se han presentado diversos factores que inciden en la preparación que se le demanda a una organización que quiera conocer estrategias y mecanismos de protección de sus datos, considerados estos como activos esenciales para la continuidad digital del negocio.

Ya no se trata solo de aplicar forensia informática cuando se detecta un incidente de seguridad sino de que la organización esté preparada para recolectar pruebas antes de que ocurra el incidente, de manera tal que pueda asegurar la confidencialidad, la integridad y la disponibilidad de dichos activos.

La metodología Forensic Readiness o Preparación Forense plantea una nueva visión sobre la recolección de evidencia digital mediante sus dos objetivos propuestos de maximizar la capacidad del entorno para reunir evidencia digital confiable y minimizar el costo forense durante la respuesta a un incidente, ya no solo para anticipar la respuesta sino también con la premisa fundamental de conservar la evidencia en perfecto estado para enfrentar procesos judiciales.

En este aspecto radica la principal diferencia con la informática forense, que es una disciplina, auxiliar de la justicia, y una aliada necesaria para enfrentar los desafíos de la seguridad informática moderna, pero que actúa luego de cometido el delito o incidente, cuando se ha incautado el dispositivo sospechoso y se han establecido puntos de pericia. En este escenario se tiende a ignorar qué ha sucedido con el objeto de la investigación antes del incidente de seguridad y antes de la decisión de realizar una investigación.

En coincidencia, tanto la forensia informática como la Forensic Readiness requieren de una correcta aplicación de métodos científicos, técnicas y herramientas para cumplimentar las etapas relacionadas con la identificación, preservación y análisis de la evidencia digital asegurando la calidad y trazabilidad de estos datos.

En el capítulo 2 se ha presentado una selección de estándares y guías más comúnmente utilizados, que si bien exhiben ciertas diferencias en sus métodos y herramientas, coinciden en aspectos sustanciales a la hora de enfrentar una investigación forense en cuanto al tratamiento de la evidencia digital respetando sus características particulares y a la necesidad de contar con recursos humanos capacitados para llevar adelante la tarea.

Ninguno de ellos incluye la preparación forense, definida como tal y como actividad previa al incidente, posiblemente porque es un concepto que ha surgido recientemente, por lo que en el apartado 3.2.3 del capítulo 3 se han descripto algunos modelos conceptuales para utilizar Forensic Readiness que podrían tomarse como base para el desarrollo de estándares o normas futuras que abarquen todo el proceso de aplicación.

En lo que respecta al poder judicial argentino, si bien se registran importantes avances en los últimos tiempos, se podrían mejorar los procedimientos contra los delitos informáticos si se contara con una normativa estandarizada de aplicación obligatoria en todas las jurisdicciones del ámbito judicial.

Otra diferencia más que surge es que en el proceso de planificación forense es necesario el compromiso de toda la organización en la detección de incidentes, en la protección de los activos y en el tratamiento de la evidencia, por lo que es recomendable su planificación con la participación de todos los sectores involucrados.

Un aspecto más a considerar es la infraestructura de almacenamiento necesaria para dar soporte al enfoque de Preparación Forense. Se deberá calcular adecuadamente la cantidad de información a resguardar para equilibrar con una solución de almacenamiento que brinde la perfomance requerida. Este punto escapa del alcance de este trabajo de tesis, pero se incluye como tema para futuros trabajos.

En el capítulo 5 se presenta un modelo de las principales etapas sugeridas para implementar la Preparación Forense, el cual puede ser adaptado a las necesidades relacionadas con características organizacionales específicas. Está basado en modelos conceptuales presentados en esta tesis, pero también toma aspectos comunes de otros modelos que refieren a la puesta en funcionamiento de sistemas de seguridad en las organizaciones. La novedad del modelo propuesto es que desde la etapa 1 toda la

organización y las acciones que se planifiquen hacen foco en los cambios necesarios para adecuarse a los requisitos de la Forensic Readiness.
El modelo tiene un alto componente de capacitación, compromiso y mejora continua para ayudar a mantener la calidad y actualización de los procedimientos que aseguren la detección de vulnerabilidades y la protección de los datos.
Para finalizar este trabajo, el capitulo 6 muestra un caso práctico de implementación de la preparación forense aplicado en el entorno de una pequeña organización ficticia que cuenta con un servidor web como principal activo para sus actividades. De estas actividades han surgido las siguientes conclusiones específicas:

- La metodología Forensic Readiness proporciona un mecanismo activo de anticipación a los incidentes en contraste con las metodologías de respuesta a incidentes de seguridad.
- En un enfoque preventivo, la integridad de los datos tratados como evidencia digital se puede asegurar con el hash que actúa como una faja digital cumpliendo la misma función que el sellado físico utilizado para resguardar dispositivos comprometidos.
- Un registro centralizado de evidencias es más fácil de implementar, mantener y proteger al estar separado de los sistemas comprometidos por incidentes. Asimismo facilita el uso de herramientas de análisis. Este repositorio, que se irá generando en la Etapa 3 del modelo propuesto, debe ser considerado como un activo de la organización.
- La trazabilidad de los datos considerados evidencia puede aumentarse implementando un control de versiones centralizado, que registre los cambios realizados sobre un archivo o conjunto de archivos a lo largo del tiempo.
- Las normas tomadas como marcos metodológicos para las pruebas, dan una guía de buenas prácticas necesarias tanto para la recolección de datos, como para su análisis y resguardo. Es de destacar que estos marcos de trabajo son adaptables a distintos tipos y tamaños de organización.
- Las herramientas de forensia informática open source, como las usadas en este trabajo, brindan el soporte necesario y eficiente para ambos enfoques, es decir para implementar un seguimiento preventivo que incluya recolección de datos, como para un análisis forense luego de un incidente de seguridad.

- Según estimaciones de diversos autores y dependiendo del activo comprometido y el volumen de información, un ataque del tipo DDoS requiere en promedio 48 horas para su mitigación, recuperación y resguardo del entorno para el análisis forense. En las pruebas de este proyecto relacionadas al tema, el servidor web que era el activo a proteger, pudo restaurarse completamente en un par de horas.
- En relación a la infraestructura mínima necesaria, hay que considerar también el valor temporal que la organización le otorgue a la información recolectada, que puede estar sujeto a políticas de la organización como así también a leyes nacionales e internacionales y/o a restricciones dadas por el propio carácter de los datos. A modo de ejemplo, y debido a las características y volumen de los archivos logs, 12 meses de resguardo puede considerarse un periodo adecuado.
- El enfoque reactivo requiere de una infraestructura de almacenamiento de menor tamaño acorde al backup periódico que se determine.
- El enfoque preventivo, y a medida que se avanza en la recolección de datos de los activos identificados, requiere una infraestructura de alta prestación. En base al activo objeto de este trabajo, que son los puntos de control del protocolo HTTP representados en su mayor parte por archivos *log,* se registró un crecimiento exponencial de los mismos a medida que ocurría el ataque DoS.
- Se debe considerar, en promedio y según las pruebas realizadas, soporte de respaldo para 500 Mb de información para el backup diario. Valor que deberá ser analizado y ajustado según la cantidad de activos y el volumen de datos que produzcan esos activos. Diversas variantes de almacenamiento se presentan como opciones en este punto, desde cloud computing hasta infraestructuras de almacenamiento conectadas a la red (NAS). Previo a una recomendación de una solución se requiere de un análisis exhaustivo de las diversas variantes para conocer sus prestaciones, ventajas y desventajas tema que trasciende el alcance de esta tesis.

Para concluir, se pone en relevancia las relaciones que han quedado establecidas a lo largo de este trabajo, especialmente que:

- Forensic Readiness y la continuidad digital de una organización se apoyan mutuamente.

- Forensic Readiness y la gestión de riesgos se complementan desde el punto de identificar los activos, sus vulnerabilidades, las medidas de protección a esos activos y en el establecimiento de políticas organizacionales relacionadas con la seguridad informática.
- A su vez, la gestión de riesgos es uno de los elementos que componen el programa de gestión de continuidad de negocio de una organización.

Por lo tanto se puede afirmar que hay una relación intrínseca entre el enfoque Forensic Readiness, la continuidad digital y la gestión de riesgos y, en base a estas relaciones se llega a la conclusión que Forensic Readiness cumple con sus objetivos principales de maximizar la capacidad del entorno para reunir evidencia digital confiable, minimizar el costo forense durante la respuesta a un incidente y minimizar el impacto en la continuidad del negocio.

Futuras Líneas de Investigación

De este trabajo de tesis se desprenden e identifican varias líneas de investigación que tienen relación directa con la Preparación Forense y se constituyen en desafíos a futuro.

En primer lugar, con relación a la infraestructura, ahondar en la cuestión de los medios de almacenamiento que requiere este enfoque y las implicancias que presenta la alternativa de Cloud Computing con respecto al tratamiento de la evidencia digital. Hay cuestiones tecnológicas y legales que impactan en la elección de una solución de nube para almacenamiento de datos privados o sensibles.

Surge una segunda línea relacionada con el ámbito organizacional, focalizando en el grado de madurez de las organizaciones de la región para adoptar este modelo de trabajo, probar versiones acotadas del modelo propuesto serviría para enriquecerlo y ajustarlo con experiencias y aportes. Asimismo diseñar un framework que permita implementar Forensic Readiness en cualquier tipo de organización puede ser una estrategia para incentivar la cultura de la protección de datos y seguridad de la información tan demanda frente a la tendencia de crecimiento sostenido de los delitos informáticos.

Analizar en profundidad que tan preparado está el sistema judicial argentino para incorporar y admitir como prueba una evidencia obtenida antes de cometido un delito puede conformar una tercera línea que ahonde en la revisión de leyes vigentes al respecto. Como así también, la cierta resistencia a aceptar herramientas open source para ser aplicadas en forensia informática que deba presentarse ante un tribunal.

Por último, surge una cuarta línea, preponderantemente técnica, relacionada con el análisis de herramientas y métodos para conservar la integridad de la evidencia digital, que en este trabajo fue realizado con hash, tal como el uso de blockchain considerando las prestaciones que ofrece para conformar una base distribuida de registro de transacciones manteniendo la seguridad, la trazabilidad y la transparencia de las operaciones.

Bibliografía

[1] RFC 2828. Internet Security Glossary. https://www.ietf.org/rfc/rfc2828.txt

[2] CISCO. Reporte Semestral 2017 https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/cisco-reporte-semestral-2017-espanol.pdf

[3] ESET Security Report Latinoamérica. https://www.welivesecurity.com/wp-content/uploads/2018/06/ESET_security_report_LATAM2018.pdf

[4] Ibragimov, Kupreev, Badovskaya, Gutnikov. Ataques DDoS, Segundo trimestre 2018. Kaspersky Lab. https://securelist.lat/ddos-report-in-q2-2018/87217/

[5] ISACA. State of Cybersecurity 2018. https://cybersecurity.isaca.org/csx-resources/state-of-cybersecurity-2018

[6] ISACA. State of Cybersecurity 2019. https://cybersecurity.isaca.org/state-of-cybersecurity

[7] Kovacich, Gerald;Boni, William. High Technology Crime Investigator´s Handbook. Butterworth Heinemann. 2000

[8] FBI CyberCrime https://www.fbi.gov/investigate/cyber

[9] Meseguer González, Juan. Aspectos legales de la prueba en una investigación pericial informática forense (2013). www.elderecho.com

[10] Código Penal de la Nación Argentina. http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16546/texact.htm

[11] Asociación Española de Normalización. https://www.une.org/

[12] ISO/IEC 27002 Information technology -- Security techniques -- Code of practice for information security controls. https://www.iso.org/standard/54533.html

[13] MAGERIT. Metodología de Análisis y Gestión de Riesgos de los sistemas de información. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

[14] Standards Australia International. HB:171 (2003) Guidelines for the Management of IT Evidence. https://www.saiglobal.com/PDFTemp/Previews/OSH/as/misc/handbook/HB171.PDF

[15] Eoghan Casey . Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. (2011) 3ra Edicion. ElSevier Academic Press.

[16] Guidelines for identification, collection, acquisition and preservation of digital evidence" ISO/IEC 27037:2012

[17] RFC 3227 Guidelines for Evidence Collection and Archiving. https://www.ietf.org/rfc/rfc3227.txt

[18] National Institute of Standards and Technology. Guide to Integrating Forensic Techniques into Incident Response. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

[19] Ministerio Público Fiscal (Argentina). Guía de Obtención, Preservación y Tratamiento de Evidencia Digital, acordada por los Ministerios Públicos del MERCOSUR. https://www.fiscales.gob.ar/wp-content/uploads/2016/04/PGN-0756-2016-001.pdf

[20] Proyecto de actualización del Código Procesal Penal de la Nación en materia de informática jurídica y criminalística digital. Dirección Nacional de Política Criminal en materia de Justicia y Legislación Penal del Ministerio de Justicia y Derechos Humanos de la Nación. http://www.pensamientopenal.com.ar/legislacion/43977-proyecto-actualizacion-del-codigo-procesal-penal-nacion-materia-informatica

[21] Tugnarelli, M.; Fornaroli, M.; Santana, S.; Jacobo, E.; Díaz, F.J. Análisis de metodologías de recolección de datos digitales. Workshop de Investigadores en Ciencias de la Computación (WICC 2017). ISBN: 978-987-42-5143-5. http://sedici.unlp.edu.ar/handle/10915/61343

[22] Piccirilli, Dario. Protocolos a aplicar en la forensia informática en el marco de las nuevas tecnologías (pericia – forensia y cibercrimen). (2016). Tesis de doctorado. Facultad de Informática. Universidad Nacional de La Plata. http://hdl.handle.net/10915/52212

[23] TAN, John. Forensic Readiness. (2001). http://isis.poly.edu/kulesh/forensics/forensic_readiness.pdf

[24] Rowlingson, Robert. A Ten Step for Forensic Readiness. (2004) International Journal of Digital Evidence. Volume 2, Issue 3.

[25] Pooe, A & Labuschagne, Les. A conceptual model for digital forensic readiness. (2012) Information Security for South Africa - Proceedings of the ISSA 2012 Conference. 1-8. 10.1109/ISSA.2012.6320452.

[26] Collie, Jan. A Strategic Model for Forensic Readiness. (2018). Athens Journal of Sciences. https://www.athensjournals.gr/sciences/2018-1-X-Y-Collie.pdf

[27] NICS, Forensics Readiness Guidelines, 2011

[28] Dauda Sule. CISA. Importance of Forensic Readiness. https://www.isaca.org/Journal/archives/2014/Volume-1/Pages/JOnline-Importance-of-Forensic-Readiness.aspx

[29] CESG. UK's National Technical Authority on Information Assurance and Cabinet Office, Government Digital Services. Good Practice Guide No. 18, (2009) Forensic Readiness,Issue No: 1.0

[30] The National Archives. Managing digital continuity. http://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/digital-continuity

[31] Tugnarelli, Mónica; Díaz Francisco Javier. Forensic Readiness: Guía de Buenas Prácticas. Libro de Actas. XXV Congreso Argentino de Ciencias de la Computación CACIC 2019. VI Workshop de Seguridad Informática, pp. 1261-1268. ISBN 978-987-688-377-1.

[32] OWASP TOP 10 https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[33] ISECOM. The Open Source Security Testing Methodology Manual https://www.isecom.org/OSSTMM.3.pdf

[34] Berners-Lee, et al. RFC 1945. HTTP/1.0. (1996). http://www.rfc-base.org/txt/rfc-1945.txt

[35] RFC 2616, Hypertext Transfer Protocol -- HTTP/1.1. 1999. https://tools.ietf.org/html/rfc2616

[36] Stenberg, Daniel. HTTP2 Explained. (2014) ACM SIGCOMM Computer Communication Review, Volume 44, Number 3.

[37] Kurose, James F., Ross, Keith W. Redes de Computadoras. Un Enfoque descendente basado en Internet. (2004), 2da. Edición, Pearson Educación.

[38] Hypertext Transfer Protocol Version 2 (HTTP/2). https://tools.ietf.org/html/rfc7540

[39] Imperva Imperva. Hacker Intelligence Initiative. HTTP/2:In-depth analysis of the top four flaws of the next generation web protocol. 2016

[40] Mónica D. Tugnarelli, Mauro F. Fornaroli, Sonia R. Santana, Eduardo Jacobo, Javier Díaz. Análisis de metodologías de recolección de datos digitales en servidores web. Libro de Actas. XXIII Congreso Argentino de Ciencias de la Computación CACIC 2017. VI Workshop de Seguridad Informática, pp. 1230-1238. ISBN 978-950-34-1539-9.

[41] KALI Linux. www.kali.org

[42] Tugnarelli, M.; Fornaroli, M.; Pacifico, C. Análisis de prestaciones de herramientas de software libre para la recolección a priori de evidencia digital en servidores web. Workshop de Investigadores en Ciencias de la Computación (WICC 2015). ISBN 978-987-633-134-0

[43] Tugnarelli, M., Fornaroli,M. Santana,S. Jacobo, E. Díaz, J. Analysis of Methodologies of Digital Data Collection in Web Serves. Communications in Computer and Information Science (Springer), Vol. 790, Pag.265. (2018) https://link.springer.com/content/pdf/bfm%3A978-3-319-75214-3%2F1.pdf

[44] National Cyber Security Centre (NCSC-UK). Denial of Service (DoS) guidance. https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection

[45] Joshila Grace, V.Maheswari, Dhinaharan Nagamalai. Analysis of Web Logs and Web User in Web Mining. International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, DOI : 10.5121/ijnsa.2011.3107 99. Department of Computer Applications Sathyabama University, Chennai, India . 2011. https://arxiv.org/ftp/arxiv/papers/1101/1101.5668.pdf

[46] NCSA Apache/ NCSA Common Log Format. https://www.loganalyzer.net/log-analyzer/apache-common-log.html

Bibliografía complementaria

[1] U.S. Department of Justice. Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition. https://www.ncjrs.gov/pdffiles1/nij/219941.pdf

[2] Digital Forensic with Open Tools. (2011). DOI: 10.1016/B978-1-59749-586-8.00001-7. Elsevier.Inc

[3] Balachander Krishnamurthy, Jeffrey C. Mogul y David M. Kristol. Key Differences between HTTP/1.0 and HTTP/1.1

[4] Cano M, Jeimy J. Computación Forense, Descubriendo los rastros informáticos. 2da. Edición. Ed. Alfaomega 2016

[5] Piattini, Mario, del Peso, Emilio. Auditoria Informática. Un enfoque práctico. 2da. Edición. Editorial Alfaomega 2001

[6] Jara, Héctor. Pacheco, Federico. Ethical Hacking 2.0 Implementación de un sistema para la gestión de seguridad. Editorial Fox Andin- Dálaga S.A. 2013

[7] Northcutt, Stephen. Novak, Judy. Detección de Intrusos. 2da. Edición. Prentice Hall. 2001

[8] Funciones Hash en la investigación forense. https://peritoit.com/2016/05/23/funciones-hash-en-la-investigacion-forense/

[9] Evidencia digital. Revista Pensamiento Penal. ISSN: 1853- 4554 http://www.pensamientopenal.com.ar/etiquetas/evidencia-digital

[10] Sallis, Ezequiel; Caracciolo, Claudio; Rodríguez, Marcelo. Ethical hacking un enfoque metodológico para profesionales. Editorial**:** Alfaomega. 2010.

Tabla de ilustraciones