IV Conferencia Científica Internacional
Universidad de las Ciencias Informáticas

Temática: Gestión de Incidentes.

METODOLOGÍA PARA LA INVESTIGACIÓN DE INCIDENTES DE SEGURIDAD EN APLICACIONES WEB

METHODOLOGY FOR THE INVESTIGATION OF SECURITY INCIDENTS IN WEB APPLICATIONS

Rafael Soto Pineda [1]

[1] Universidad de Ciencias Informáticas UCI.

[*] Autor para correspondencia: rspsuperman@gmail.com

RESUMEN

El rápido crecimiento que ha tenido la utilización de las aplicaciones web ha propiciado un aumento considerable de riesgos de seguridad que atentan contra la disponibilidad, integridad y confidencialidad de la información. Los softwares inseguros debilitan cada día las finanzas, salud, defensa, energía, y otras infraestructuras críticas de cualquier país a nivel mundial. No importa cuán desarrollados estén las tecnologías, a medida que el software se convierte en algo necesario, crítico, complejo e interconectado, la dificultad de lograr seguridad en las aplicaciones web aumenta exponencialmente. Este ritmo vertiginoso del desarrollo de aplicaciones web actuales, incrementa aún más el riesgo de no descubrir vulnerabilidades de forma rápida y precisa, y de esta manera poder realizar una gestión más eficiente a los incidentes de seguridad generados en estas aplicaciones web. Por ello, se requiere la adopción de mecanismos para el enfrentamiento a los problemas de seguridad que se presentan diariamente en las aplicaciones

web, comenzando desde la adopción e inclusión de elementos de seguridad a lo largo del ciclo de desarrollo de una aplicación, hasta la detección, prevención y corrección de posibles vulnerabilidades en nuestras aplicaciones web. Indispensable resulta para cualquier especialista de seguridad el estudio de las metodologías propuestas por las principales entidades a nivel mundial en estos temas. Para luego nos permita conformar una metodología adaptable y flexible que nos proponga cómo gestionar e investigar las violaciones de seguridad en aplicaciones web.

Palabras clave: aplicaciones web, riesgos, incidentes, seguridad, información, vulnerabilidades, gestión.

ABSTRACT

The rapid growth in the use of web applications has led to a considerable increase in security risks that threaten the availability, integrity and confidentiality of information. Insecure software's weaken every day the finances, health, defense, energy, and other critical infrastructures of any country worldwide. No matter how developed the technologies are, as software becomes necessary, critical, complex and interconnected, the difficulty of achieving security in web applications increases exponentially. This dizzying pace of development of current web applications further increases the risk of not discovering vulnerabilities quickly and accurately, and thus being able to more efficiently manage security incidents generated by these web applications. Therefore, the adoption of mechanisms to deal with the security problems that occur daily in web applications is required, starting from the adoption and inclusion of security elements throughout the development cycle of an application, until detection, prevention and correction of possible vulnerabilities in our web applications. Indispensable for any security specialist is the study of the methodologies proposed by the main entities worldwide on these topics. Then, it allows us to form an adaptable and flexible methodology that proposes how to manage and investigate security breaches in web applications.

Key words: *web applications, risks, incidents, security, information, vulnerabilities, management.*

Introducción

La historia de Internet nace con el desarrollo de las redes de comunicaciones que permitieron la comunicación entre computadoras y usuarios desde diferentes ubicaciones físicas. A partir de la década de los 80 comenzó una expansión e incorporación a internet de diversas redes de Europa y del resto del mundo, poco después en los 90, se introdujo por primera vez la Word Wide Web (www), que se hizo común y con ello se crearon las bases del protocolo de transmisión HTTP ("Hypertext Transfer Protocol"), el lenguaje de documentos HTML ("Hypertext Markup Lenguage") y el concepto de URL (Uniform Resource Locator). Para entonces el impacto de esta naciente red en el mundo ya se hacía notar, por lo que fue necesario mejorar las paginas estáticas desarrolladas en HTML, dando surgimiento al código HTML dinámico, capaz de actualizar los formularios y las bases de datos. La Real academia española incluyó el vocablo "internet" como un sustantivo en 2006 y la definió como una "red informática mundial, descentralizada, sobre la base de protocolos especiales de comunicación". En especial el protocolo TCP/IP ("transmisión Control Protocol") el cual se encarga de realizar el intercambio de información.

A lo largo de los años esta gran red de comunicación se ha extendido a todos los rincones del mundo, con el propósito de mantener y extender su desarrollo para todas las personas interconectadas. Convirtiéndose así en un medio de comunicación masiva a nivel mundial. Según la revista digital "Digital Around The Word" publicó que hasta el año 2019 existían aproximadamente 4.388 mil millones de internautas en todo el mundo. Es una clara realidad, que el aumento del uso de internet se debe a varias ventajas como son el dinamismo de la información disponible en internet, la aparición y actualización constante de nuevos sitios web, es universal, anónimo, económico, rápido y de fácil uso. Destacar otras ventajas como la realización de transacciones económicas, generación de datos desde cualquier lugar, gestión de correos electrónicos, entre otras muchas ventajas, considerada por muchos analistas como una inagotable fuente de información almacenada.

En los primeros días de internet, solo existían sitios web consistentes en repositorios de información contenida en documentos estáticos, además del surgimiento de los navegadores web como un medio de recuperación y visualización de dichos documentos. El flujo de información era en un único sentido. La mayoría de los sitios no autenticaba usuarios debido a que cada usuario era tratado de la misma manera y le era presentada la misma información. Cualquier amenaza de seguridad emergente de hospedar un sitio web estaba principalmente relacionada con las vulnerabilidades del servidor web. Si un atacante comprometía un servidor web, generalmente no lograba

acceso a la información sensible, puesto que ya estaba abierta al público, solo restaba al atacante modificar el código fuente del sitio o aprovechar el almacenamiento del servidor.

Al igual que con cualquier tecnología nueva, las aplicaciones web vienen acompañadas con una nueva variedad de vulnerabilidades de seguridad. El conjunto de los defectos que se detectan con mayor frecuencia ha evolucionado a lo largo del tiempo, los nuevos ataques están concebidos de forma tal que resulta imposible considerarlos al momento del desarrollo de las aplicaciones, lo que no quiere decir que los programadores de web no tengan que cumplir con ciertos estándares relacionados a métricas de desarrollo seguro de aplicaciones web.

Al hablar de aplicaciones web la referencia debe de ser a seguridad lógica y física, tal es el caso de la norma ISO/IEC 17799 (International Organization for Standardization / International Electrotechnical Commission) que evalúa el nivel de protección de un sistema informático, analizando la confidencialidad, integridad y disponibilidad. Las aplicaciones web, por definición, permiten el acceso de usuarios a recursos centrales tal como al servidor web y el cual permite el acceso a otros servidores de base de datos. Con los conocimientos y la implementación correcta de medidas de seguridad, se pueden proteger los recursos, así como proporcionar un entorno seguro en el cual los usuarios trabajen cómodos con su aplicación.

Con la realización de este trabajo se pretende el desarrollo de procesos de gestión de eventos de seguridad, a partir del estudio de estándares y normas que agrupan un conjunto de elementos sobre la Seguridad en Aplicaciones Web. Existen hoy, varios modelos de gestión de Incidentes, en los cuales no se especifica de manera particular el trabajo a realizar con los eventos de seguridad generados en servidores web, páginas web, gestores de contenido, foros, correos, etc. Resulta indispensable tener identificado cuales son las vulnerabilidades que pudieran existir y la manera en que los atacantes la explotarían. La realización de un buen análisis de riesgo y vulnerabilidades permitirá a los especialistas de redes, identificar cuáles son los problemas de seguridad, establecer un perímetro de seguridad en caso de no poder llevar a cabo una gestión de parches de seguridad en los servicios web, realizar una capacitación sobre temas de seguridad informática aplicado al marco estrecho de las Aplicaciones Web.

Materiales y métodos o Metodología computacional

Campo de acción

Esta investigación se ubica, dentro del área del conocimiento de la Seguridad Informática, en el área específica de metodologías para la Gestión de Incidentes de Seguridad en Aplicaciones Web.

Donde se plantean los siguientes campos de acción:

- Estudio de estándares Internaciones de Seguridad en Aplicaciones Web.
- Análisis cualitativo.
- Análisis cuantitativo.
- Identificación de riesgos y vulnerabilidades.
- Gestión de Incidentes de Seguridad.

Tipo de investigación

- **Exploratorias:** A pesar del conocimiento adquirido en estos últimos años sobre el desarrollo vertiginoso de las Aplicaciones Web, se impone el estudio y la investigación sobre las vulnerabilidades que pudieran convertirse potencialmente en ataques a dichas aplicaciones.

- **Descriptivos:** Con la investigación más a fondo sobre las vulnerabilidades que pudieran tener las Aplicaciones Web hoy día, se busca un equilibrio constante entre amenazas, riesgos e incidentes de seguridad, se busca determinar con más exactitud dentro de un Sistema Integral de Gestión de Incidentes Informáticos, los que tuvieran que ver directamente en las Aplicaciones Web.

Hipótesis

La aplicación de una metodología para la investigación de Incidentes de Seguridad en Aplicaciones Web, sobre la base de los estándares Internacionales en Seguridad de Aplicaciones Web y su integración a un Sistema de Gestión de Incidentes Informáticos, identificará de manera particular ataques y vulnerabilidades en las Aplicaciones Web, así como la disminución de Incidentes de Seguridad.

Métodos de investigación

Para la realización de la propuesta metodológica, el autor tuvo en cuenta varios métodos científicos que permitieron una mejor organización en el trabajo y poder obtener resultados aceptables de acuerdo a las necesidades previstas. Estos métodos se dividen en Empíricos y Teóricos, los cuales se describen a continuación.

Métodos Teóricos:

- **Histórico – Lógico:** se utilizó para determinar los antecedentes relacionados con la seguridad de las Aplicaciones Web desde su surgimiento y su estrecha relación con los elementos de la Seguridad Informática.

- **Analítico – Sintético:** se utilizó para la investigación de las vulnerabilidades en Aplicaciones Web, así como las amenazas que enfrentan dichas aplicaciones en el mundo de hoy. Permitió la conformación de un modelo de gestión de eventos de seguridad, específicamente en Aplicaciones Web.

- **Hipotético – Deductivo:** se utilizó para el estudio y análisis de otros modelos de gestión a la seguridad en Aplicaciones Web, así como en la elaboración de la hipótesis.

Métodos Empíricos:

- **Observación:** se utilizó para conocer las vulnerabilidades más comunes que pudieran contener las Aplicaciones Web de cara a internet, cómo se pudieran prevenir, detectar, evitar explotación y establecer la protección necesaria de las Aplicaciones Web y toda su infraestructura.

Resultados y discusión

En este trabajo se propone un modelo metodológico para la correcta gestión de un incidente de seguridad en Aplicaciones Web. Para esto, se tomará como guía las metodologías sobre ataques a Aplicaciones Web por algunas de las organizaciones internaciones, que además son pioneras en cuanto al trabajo con la seguridad de dichas Aplicaciones, así como lo planteado por el Ministerio de Comunicaciones de la República de Cuba en su Resolución

128 del año 2019 sobre Incidentes de Seguridad. Por último, se abordarán elementos sobre el análisis de riesgo y vulnerabilidades, como parte de la prevención a la ocurrencia de nuevos incidentes de seguridad en el futuro.

Propuesta metodológica para la Gestión de un Incidente de Seguridad en Aplicaciones Web

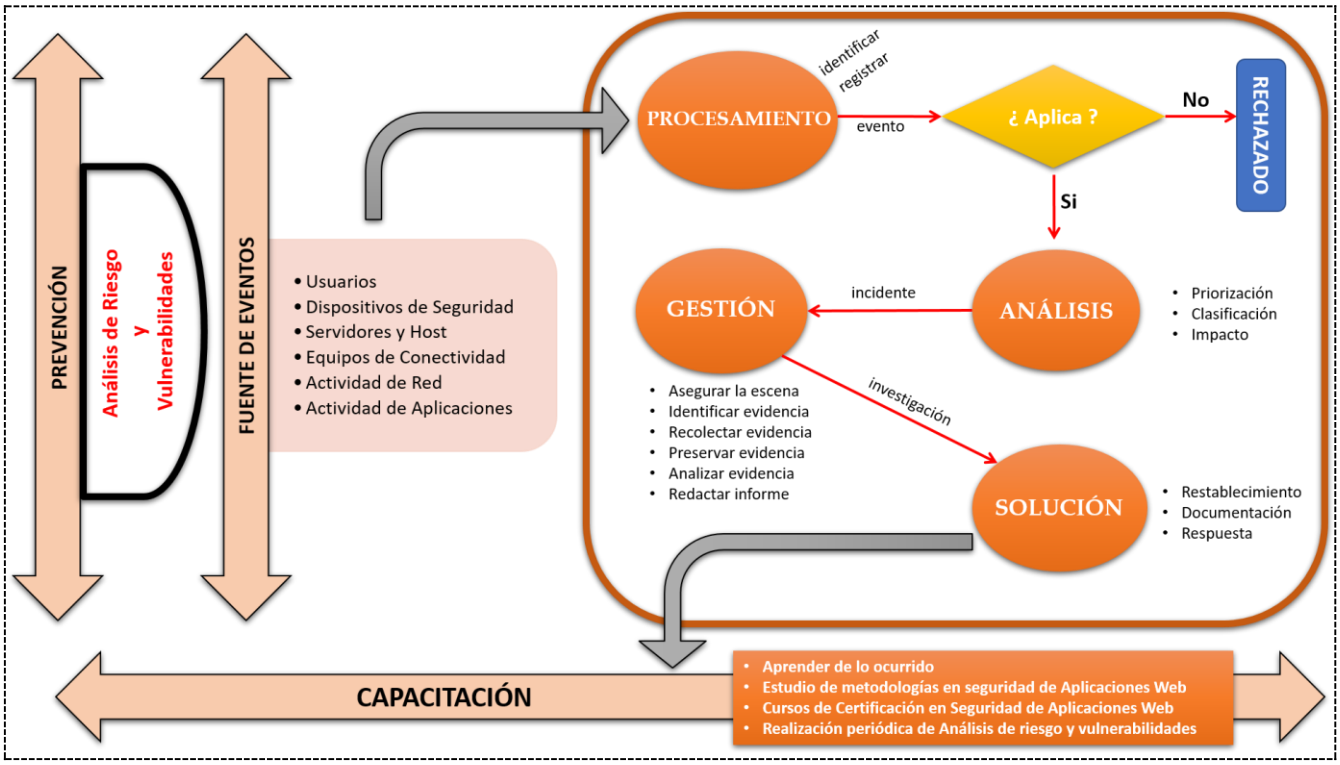

Figura 1. *Metodología para la gestión de incidentes de seguridad en aplicaciones web.*

Como se puede apreciar el esquema anterior reúne un conjunto de elementos que, relacionados entre sí, conforman la metodología que se propone aplicar a la Gestión de Incidentes de Seguridad en Aplicaciones Web. Esta propuesta tiene como objetivo, la de prevenir, analizar, identificar, procesar e investigar eventos de seguridad que pudieran convertirse en incidentes, dar solución y proponer elementos de capacitación en la prevención de amenazas futuras.

Señalar, que la propuesta aplica lo relacionado a elementos y procedimientos estudiados en los estándares de seguridad mostrados al principio de este capítulo, así como los elementos abordados en la **Resolución 128** del 2019 por el Ministerio de Comunicaciones de la República de Cuba y que aprueba el Reglamento de Seguridad de las

Tecnologías de la Información y la Comunicación. Esta resolución, en su **Capítulo VI**, sobre Incidentes de Seguridad plantea que [7]:

Artículo 45: La estrategia que se formule en la entidad ante cualquier incidente o violación de la seguridad es consecuente con sus objetivos básicos, donde se define el Plan de Prevención de Riesgos.

Artículo: 46: Los procedimientos para la gestión de incidentes y violaciones de seguridad de las TIC, tienen los requisitos de reportar de inmediato, la comunicación con los afectados e involucrados, el análisis y la identificación de las causas, el registro de los eventos vinculados, la recolección y preservación de las trazas de auditorías, la planificación y la implementación de medidas para prevenir la recurrencia.

Artículo 47: Ante cualquier incidente que afecte la seguridad de las TIC de una entidad, su dirección designa una comisión, integrada por especialistas no comprometidos directamente con este hecho, encargada de realizar las investigaciones necesarias para esclarecer lo ocurrido, determinar el impacto, precisar los responsables y proponer la conducta a seguir.

Artículo 48: La dirección de cada entidad queda obligada, al producirse un incidente o violación de la seguridad informática, reportarlo inmediatamente a la OSRI (en este caso el órgano encargado de realizar la investigación en Cuba) y la instancia superior de la entidad.

Con el desarrollo de esta metodología, se propone su aplicación a cuatro fines que se describen a continuación:

- Fines Preventivos
- Fines Correctivos
- Fines Probatorios
- Fines Auditores

Fines preventivos: Puede ayudar a prevenir incidentes de seguridad. En este caso los especialistas de seguridad utilizarán herramientas para verificar y auditar que los sistemas y aplicaciones cumplen con los objetivos descritos en sus estándares de seguridad. Los resultados de estos estudios aportarán información valiosa de cara a mejorar la seguridad de los mismos.

Fines correctivos: En caso de la detección oportuna de posibles fallos de seguridad informática, se debe de iniciar automáticamente un análisis entre los especialistas de seguridad, con el objetivo de corregir los fallos detectados e

implementar las soluciones que sean más convenientes para evitar que un cliente malintencionado pueda poner en riesgo los sistemas y aplicaciones.

Fines probatorios: Esta finalidad permite, que tras el registro de un incidente informático, se pueda recabar información sobre la intrusión en el sistema, descubrir qué daños se han producido, robo de información o destrucción de la misma, entre otros. Incluso se pudieran descubrir él o los causantes del incidente, su origen, el alcance de la afectación a otros equipos o aplicaciones. Finalmente, con todos los datos recogidos, organizados y bien preservados, se pueden entonces presentar como evidencias concretas del delito, aportando pruebas legales y válidas ante cualquier proceso penal.

Fines auditores: Relacionado con los fines correctivos, se pueden programar auditorías de seguridad, que llevan a cabo entidades especializadas en temas de seguridad informática y ciberseguridad, que verifiquen periódicamente el cumplimiento de todos los requisitos de seguridad implementados en los sistemas y aplicaciones informáticas, además de velar por la ejecución de buenas prácticas en el manejo de la seguridad por parte de los administradores y responsables de seguridad informática.

Desarrollo del proceso de Prevención

Como parte del proceso de prevención ante amenazas, riesgos y vulnerabilidades de seguridad en aplicaciones web, se abordan un conjunto de elementos que conforman un análisis de riesgo y vulnerabilidades.

Una **amenaza** es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de una aplicación web. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestra aplicación. Las amenazas pueden proceder de ataques (fraude, robo, virus), eventos físicos (incendios, catástrofes) o simplemente negligencias de servicio y malas decisiones (mal manejo de contraseñas, no usar cifrado). Por tanto, las vulnerabilidades son las condiciones y características propias de cualquier aplicación web que la hacen susceptible a las amenazas. Siempre que exista una vulnerabilidad, podemos afirmar con total seguridad, que habrá alguien que intentará explotarla, es decir, sacar provecho de su existencia.

De igual manera, es interesante introducir el concepto de **riesgo**, definido como la probabilidad de que se produzca un incidente de seguridad, materializándose una amenaza y causando pérdidas o daños. Se mide, como el producto de la probabilidad de que la amenaza se materialice aprovechando una vulnerabilidad y el impacto de los posibles daños.

Desarrollo del proceso de Gestión del Incidente de Seguridad

Para la realización del proceso de gestión, se dividirá en cinco etapas, con el objetivo de lograr un proceso de investigación exitoso. Se recalca la importancia de preservar el entorno de las pruebas, no modificar el escenario encontrado, el cómo guardar de forma segura las pruebas, su transporte y conservación. Centrarse en cómo analizar las pruebas para obtener el máximo rendimiento de las mismas y poder esclarecer todo hecho ocurrido. Finalmente, la importancia de la confección de un buen informe claro, conciso y de utilidad, capaz de ser traducido a una persona no entendida en el tema y pueda comprender lo ocurrido.

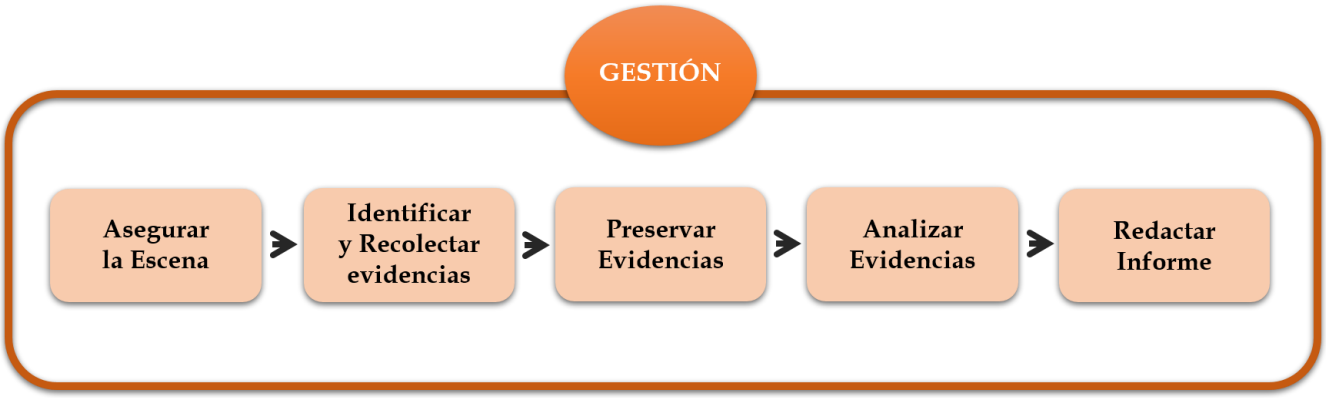

Figura 2. *Etapas del proceso de gestión.*

Como se puede apreciar en la figura anterior, se muestra la relación entre una etapa y otra, en cada una de ellas se darán las mejores comendaciones y los pasos a seguir para no cometer ningún error en las investigaciones. Señalar que no todas las investigaciones se producen ante hechos criminales, por tanto, esta metodología se aplica para varios fines, como se abordó anteriormente, puede ser simplemente una auditoría, reconstrucción de un sistema dañado producto de un desastre natural, un proceso de aprendizaje o la toma de medidas para que no se produzca un determinado problema.

A continuación, se describen los procedimientos de cada etapa:

Etapa I. Asegurar la escena

El investigador no solo se tiene que centrar en un análisis técnico de los activos implicados en el incidente, también debe asegurarse que la escena donde se ha producido o se está produciendo dicho incidente no haya sido alterada, desde el descubrimiento del mismo hasta el inicio de su análisis. Todos los implicados en la investigación deben ser conscientes que cualquier acto que lleven a cabo puede comprometer la investigación provocando consecuencias posteriores, no ejecutar acciones deliberadamente sin claridad. El trabajo debe realizarse en equipo, consensuar las acciones y llevar un registro de las mismas. Es recomendable realizar fotografías del entorno afectado, para evidenciar el estado original de la escena, identificando así el perímetro de la escena a analizar y protegiéndolo de accesos no autorizados.

Una vez dentro del perímetro de seguridad hay que proteger todo tipo de evidencias y huellas (informes de procesos, mensajes, logs de sistemas y aplicaciones) que pueda haber en los servidores implicados. Anotar la fecha y hora de los servidores implicados, que no necesariamente tiene que coincidir con la real, importante para luego poder construir una línea de tiempo con todos los sucesos ocurridos. La captura de los datos debe realizarse de manera tal, que no se manipulen los servidores y provocar la ejecución automática de algún proceso que atente contra las trazas registradas en los equipos. Registrar las entradas y salidas a los equipos, servidores y aplicaciones web.

Con respecto a la desconexión de los servidores web o Base de Datos, se pudieran producir alteraciones en el proceso de investigación, por lo tanto, se debe documentar exactamente las acciones realizadas, así como su justificación. En cuanto a la desconexión de red, si se realiza, se logra que un determinado hecho siga ejecutándose, por ejemplo, una descarga de datos no autorizada o el borrado remoto de información, trazas y configuraciones en los servidores, pero también se corre el riesgo de perder información sobre posibles conexiones que den el origen del incidente o indicios del atacante. De igual forma habrá que valorar la desconexión eléctrica de los equipos. Una desconexión eléctrica evitará que algún proceso continúe ejecutándose y escribiendo es disco, pero también podría provocar alguna escritura de datos si se ejecuta algún proceso maligno con programación ante fallos eléctricos. También se podría haber planificado un borrado de datos en caso de la desconexión eléctrica.

Una vez finalizada la primera Etapa, y con la escena bien asegurada teniendo en cuenta todos los puntos expuestos anteriormente, se podrá pasar a la segunda Etapa.

Etapa II. Identificación y Recolección de Evidencias

Para una mayor explicación subdividiremos la Etapa en dos apartados, por un lado, la parte relacionada a la identificación de las evidencias y por otro lado la recolección de las mismas.

Identificación de Evidencias:

En este apartado hay que tener en cuenta una serie de principios a cerca de la identificación de las evidencias y más específicamente sobre la ***volatilidad*** de las mismas. Es vital conocer qué datos son más o menos volátiles, identificarlos correctamente y proceder a su recolección.

Se entiende por volatilidad de los datos el periodo de tiempo en el que estará accesibles en los servidores y ficheros de registro:

- Registros contenidos en la memoria caché de los clientes, navegadores web.
- Tablas de enrutamiento de equipos de redes, tablas de procesos en ejecución en servidores web y bases de datos.
- Información temporal del kernel de los servidores.
- Datos contenidos en los discos duros.
- Registros Logs del Sistema Operativo.
- Registros Logs del servidor web.
- Registros Logs del Servidor de Bases de Datos.
- Registros Logs servidores proxys, IDS de red y de Host.
- Registros Logs de Firewalls de Aplicaciones y Servicios.
- Configuración Física y topología de la Red donde se encuentra la Aplicación Web.
- Otros documentos de interés, como las carpetas de administración de aplicaciones y servicios.

Una vez identificada todas las evidencias posibles, de acuerdo al orden de volatilidad establecido por los investigadores, se procede a seleccionar cuales serán de utilidad para el proceso.

Recolección de Evidencias.

Copia bit a bit de los discos que se quieran analizar, pertenecientes a los servidores web y base de datos (se propone el proceso de clonado de los discos duros). Esto incluye todos los archivos del disco, los temporales, los ocultos, los de

configuración, hasta los eliminados. Esta copia se llevará a cabo sobre un soporte, que previamente fue sometido a un proceso de borrado seguro a bajo nivel, para no correr el riesgo de contaminación con otros casos anteriores. Una vez copiada la información se debe verificar la integridad de la misma, o sea, calcular el hash de la copia. Con la primera copia ejecutada y comprobada se procede a realizar una segunda y una tercera copia, con el mismo rigor que en el proceso de la primera copia, como se muestra en la siguiente figura.

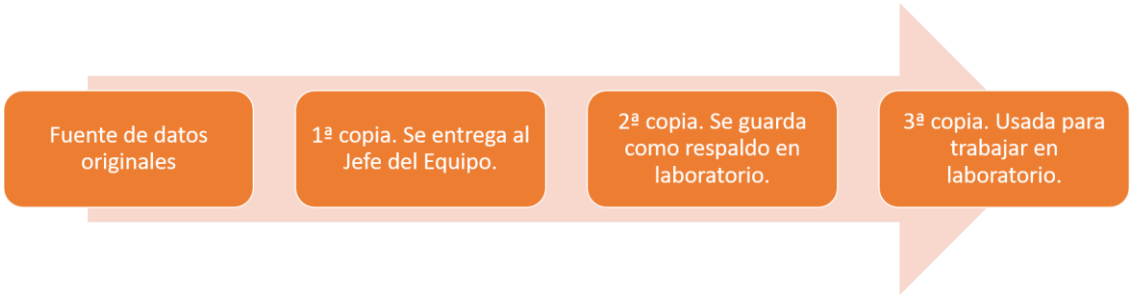

Figura 3. *Ciclo de la recolección de evidencia.*

Etapa III. Preservación de las Evidencias

Una mala preservación de las evidencias, puede invalidar toda la investigación que se lleva a cabo. La cadena de custodia es el procedimiento controlado aplicable a las evidencias relacionadas con el suceso, desde el momento en que se encuentran en la escena hasta su análisis en el laboratorio. La finalidad de la cadena de custodia es evitar cualquier tipo de manipulación, sea o no malintencionada, tener un control absoluto sobre todos los elementos incautados, quién los ha manipulado, cómo lo ha realizado, porqué los ha manipulado, para qué lo ha hecho y cuando ha tenido lugar dicha manipulación.

Se tendrá en cuenta el traslado seguro de la evidencia hasta el laboratorio, así como su vía de transporte. Una vez que se asuma el lugar que funcionará como laboratorio, este deberá tener un mínimo de condiciones de seguridad, un almacenamiento con control absoluto de accesos físicos y lógicos, evitar los trabajos en sitios húmedos, con temperaturas extremas o con exceso de polvo y suciedad, respaldo energético ante fallas de corriente eléctrica, facilidad de conectividad, recursos para replicar los servidores web y bases de datos. También deberá de existir un registro de todos los lugares donde se ha trabajado con la evidencia, así como el especialista encargado del transporte y el que realiza los trabajos de laboratorio.

Etapa IV. Análisis de las Evidencias

La etapa de análisis no termina hasta que se pueda determinar qué o quién causó el incidente, cómo lo hizo, qué afectación ha tenido en la aplicación web. Esta etapa se considerará como el núcleo principal de la investigación. Antes de comenzar el análisis, es importante recordar que no se deben trabajar con los datos originales, los resultados parciales que se obtengan han de ser verificables y reproducibles de manera qué, en caso necesario se pueda montar un entorno simulado para demostrar de forma práctica los resultados en base a las evidencias. Disponer además de toda documentación adicional al proceso de investigación.

- Uso de firewall.
- Uso de IDS.
- Uso de Proxys.
- Herramientas de Seguridad.
- Sistemas Operativos implementados.
- Servidores web.
- Servidores de Bases de Datos.
- Tipo de Aplicación Web.
- Marco de Trabajo Utilizado.
- Lenguajes de Programación web.
- Gestores de Contenido.
- Servidores de Correo.
- Equipos de conectividad.
- Infraestructura de Servicio.
- Infraestructura de Aplicaciones.
- Tecnología de virtualización.
- Hardware.
- Topología de la red implementada.
- Ubicación de los dispositivos implicados en la red.
- Conexiones internas y externas a la red.
- Configuraciones específicas que puedan ser de interés para el especialista que analiza.

Para ayudar al desarrollo de esta Etapa, se dividirá en varios puntos:

- Preparar un entorno de trabajo adaptado a las necesidades del incidente.
- Reconstruir una línea temporal con los hechos sucedidos.
- Determinar las acciones que llevó a cabo el atacante.
- Identificar el autor o autores del hecho.
- Evaluar el impacto causado y si es posible recuperar el sistema.

Preparar un entorno de trabajo adaptado a las necesidades del incidente

En este punto se debe decidir si el proceso de análisis se realizará en caliente o en frío. En caso de un análisis en caliente se hará la investigación sobre los discos, sistemas y aplicaciones originales, lo que conlleva cierto riesgo y por ende es necesario tomar todas las precauciones posibles, puesto que cualquier error pudiera invalidar las pruebas y provocar la destrucción total o parcial del sitio web.

En cambio, si se opta por un análisis en frío, lo más sencillo sería preparar un entorno virtual con los mismos sistemas operativos, servidores web, bases de datos y sitios web, a partir de las copias que previamente que se realizaron. En este caso se ejecutan acciones de escaneos, detección y explotación de vulnerabilidades, trazas y registros sobre comportamientos sospechosos de procesos.

Se propone el uso de herramientas de seguridad tales como:

- Nmap.
- Wireshare.
- OWASP
- Armitage
- Compendio de Herramientas del Sistema Kali Linux.

Reconstruir una línea temporal con los hechos sucedidos

Se ubican los acontecimientos que van teniendo lugar a lo largo de todo el proceso de investigación. Para empezar, se debe determinar la fecha y hora de instalación de los sistemas operativos, así como la instalación de servidores web, bases de datos, publicación de sitios web, ejecución sistemática de procesos del sistema. La fecha de creación y

modificación de los archivos de configuración y carpetas del directorio raíz en todas las particiones de los equipos y de los sitios web. Comprobar si se han creado usuarios o si existió alguna elevación en la escala de privilegios.

Teniendo ya los datos iniciales del sistema, se procede a profundizar en la búsqueda de información en los ficheros que se ven a simple vista. Localizar qué programas se instalaron recientemente y que cambios realizaron en el sistema. Lo más probable es que si estamos en presencia de un programa maligno o la ejecución de un script con códigos dañinos, estos se alojen en rutas poco comunes, pudieran mezclarse con los archivos temporales, o con los archivos y librerías del sistema operativo o en la infraestructura de ficheros de una aplicación web publicada en nuestra red.

Sobre los archivos, no todos están a la vista. Se puede encontrar información en temporales, ocultos, borrados o usando técnicas de recuperación. Habitualmente los sistemas operativos ofrecen la opción de visualizar los archivos ocultos, sería de mucha utilidad activar estas opciones para detectar posibles elementos ocultos y extensiones desconocidas.

Sobre los archivos borrados, se utilizarán programas especiales capaces de recuperar aquellos datos que se hayan eliminado del disco, pero sobre los cuales no se ha practicado ninguna sobreescritura. Es posible que el atacante elimine archivos o registros con el afán de esconder las huellas de lo que ha ocurrido.

Es posible que el atacante utilizara técnicas de enmascaramiento para ocultar ficheros ejecutables en ficheros de audio, video, imagen o cualquier otro tipo de extensión. Para posteriormente robar o destruir poco a poco la aplicación web en su totalidad.

Determinar las acciones que llevó a cabo el atacante

Primero, se comprueba la integridad de los datos, del sitio web y el sistema de fichero de los servidores. Analizar los eventos arrojados por las herramientas utilizadas y detectar si se ha producido la explotación de alguna vulnerabilidad en aplicaciones web, dígase inyección de código, pérdida de autenticación, etc.

Tener en cuenta los siguientes aspectos:

- Ficheros de configuración y despliegue de servidores web, base de datos y páginas web.
- La gestión de la identidad.
- Los métodos de autenticación.
- Los métodos de autorización.
- La gestión de sesiones.

- La validación de entradas.
- El manejo de errores.
- Mecanismos criptográficos.
- Métodos de auditorías en la propia aplicación.

Revisar la tabla de procesos para saber qué ejecutables están en uso y qué librerías se ven involucradas. A menudo, cuando se analiza la tabla de procesos, se observan procesos en ejecución aparentemente inofensivos, habituales y legítimos. No es extraño que determinados procesos con fines malintencionados se camuflen con procesos legítimos.

Identificar el autor o autores del hecho

Partiendo de la información recopilada en los logs, buscar indicios que apunten a direcciones IP de origen, códigos maliciosos, referencias a sitios web utilizados por el atacante, con el objetivo de determinar si el ataque se produjo desde la red interna o desde la red externa, en este punto cumple un papel importante el uso de firewall y proxys, así como IDS de red. Es de conocimiento, que en ocasiones el atacante utiliza técnicas para distribuir los ataques (empleo de botnet) o falsear la dirección IP (pool de direcciones, nat de direcciones de host y de red).

Evaluar el impacto causado y si es posible recuperar el sistema

El impacto causado se puede calcular en base a distintos factores y no hay un método único para su cálculo, ni una fórmula que refleje con total exactitud un importe económico. Aún así, para estos cálculos existen varias metodologías implementadas en el mundo. En general, cualquier incidente ocurrido, devengará en muchos gastos económicos que habrá que cuantificar, en función de los elementos de la infraestructura de soporte y de servicio que fueron afectados tras el suceso. En ocasiones, el costo económico se verá representado en el remplazo de un elemento de hardware o software que ha quedado inservible tras un ataque, pero también se verá representado por el tiempo empleado por los administradores de servicio y especialistas de seguridad en restablecer el correcto funcionamiento de los sistemas y servicios, dígase desde la reinstalación de sistemas operativos, la correcta configuración de los elementos de seguridad en las aplicaciones, hasta la actualización de dichas aplicaciones y la incorporación de parches de seguridad ante vulnerabilidades conocidas.

En otras ocasiones, los daños pueden deberse al robo de información sensible, datos bancarios, cuentas financieras, contraseñas, y otras de interés para dañar la imagen de la entidad comprometida.

Dada la experiencia reciente de los especialistas en seguridad, el elemento más expuesto a ataques sería el sitio web, debido a que realiza la primera interacción con los clientes, y es además por donde los atacantes tratan de vulnerar en primera opción dicha seguridad. Por lo que se recomienda, ante cualquier implementación de sitios web, gestores de contenido, servidores de correo, etc, asegurar uno o varios espejos, que garanticen el restablecimiento íntegro tanto de la configuración del sitio web, como de su contenido.

Etapa V. Redacción de Informes

La última fase de un análisis forense queda para redactar los informes que documenten los antecedentes del evento, todo el trabajo realizado, el método seguido y las conclusiones e impacto que se ha derivado producto del incidente.

Para ello se propone la rección de dos tipos de informes, el informe ejecutivo y el técnico. En esencia, en ambos informes se exponen los mismos hechos, pero variando su enfoque y el grado de detalles con que se explican los sucesos.

Informe Ejecutivo.

Se usará un lenguaje claro y sin tecnicismo, se debe evitar el uso de terminologías propias de la ciencia en ingeniería y expresiones confusas para las personas no duchas en el tema. Será un resumen de toda la tarea que sea llevado a cabo con las evidencias digitales. Aunque será un documento de poca extensión, éste en su redacción deberá tener los siguientes puntos:

- **Motivos de la Intrusión.**
  - ¿Porqué se ha producido el Incidente?
  - ¿Qué finalidad perseguía el atacante?
- **Desarrollo de la Intrusión.**
  - ¿Cómo lo ha logrado?
  - ¿Qué ha acciones ha realizado sobre los sistemas y aplicaciones?
- **Resultados del Análisis.**
  - ¿Qué ha pasado?
  - ¿Qué daños se han producido o se pronostican?
  - ¿Es denunciable?
  - ¿Quién es el autor o los autores?

- **Recomendaciones.**
    - ¿Política a seguir?
    - ¿Cómo protegerse para evitar la repetición futura de tales hechos?

Informe Técnico.

En este informe, el público final será de un perfil técnico y con conocimientos de los temas que se exponen. Se detallarán todos los procesos, los programas utilizados, las técnicas empleadas, etc. Crear un documento que sirva como guía para repetir el proceso en caso de la ocurrencia de hechos similares. Este informe deberá tener los siguientes puntos:

- Antecedentes del Incidente.
    - Descripción de cómo se encontraba el sistema antes del incidente.
- Recolección de Datos.
    - ¿Cómo se ha llevado a cabo el proceso?
    - ¿Qué se ha recolectado?
- Descripción de la Evidencia.
    - Detalles técnicos de las evidencias recolectadas, su estado y contenido.
- Entorno de trabajo del análisis.
    - ¿Qué herramientas se han utilizado?
    - ¿Cómo se han utilizado?
- Análisis de la Evidencia.
    - Se deberá informar del sistema analizado aportando datos como, las características de los sistemas operativos, aplicaciones instaladas, servicios en ejecución, vulnerabilidades detectadas, configuración de seguridad en las aplicaciones y la metodología utilizada.
- Descripción de los resultados.
    - ¿Qué herramientas y técnicas ha usado el atacante?
    - ¿Qué alcance ha tenido el incidente?
    - Determinar el origen del mismo y como se ha encontrado.
- Presentar la línea temporal de los hechos ocurridos con todos los detalles.

- Redactar unas conclusiones con valoraciones que se crean oportunas, luego de la consensuada opinión del 100 % de los especialistas que participaron en la investigación.
- Dar un conjunto de recomendaciones sobre cómo proteger al sistema para evitar futuros incidentes de seguridad, y sobre todo cómo actuar en caso de la ocurrencia de otros.

Conclusiones

Es una realidad la cantidad creciente de usuarios que hacen uso de internet, y la tendencia actual de presentar la información de los servicios ofrecidos a los usuarios a través de páginas web, así como el almacenamiento compartido de datos sensibles en la gran red de datos. En la actualidad existe una brecha de conocimiento en los campos de seguridad de la información y la gestión de incidentes de seguridad, muy puntualmente en aplicaciones web. Es esencial que los especialistas en seguridad, en sistemas y redes, comprendan la necesidad de lograr una elevada preparación y capacitación ante situaciones críticas producidas por amenazas y ataques informáticos de cualquier naturaleza.

En este trabajo, se abordaron elementos referidos a las aplicaciones web, con el objetivo de concientizar a los especialistas y administradores de servicio en la necesidad de brindar la mayor seguridad posible a las aplicaciones web publicadas. Se tomó como referencia el marco teórico estudiado en el capítulo 1, para luego fomentar las bases de la realización de una propuesta metodológica, que reuniera todos los elementos, que permitan la investigación eficiente de un incidente de seguridad. Se describió de manera detallada el desarrollo del proceso de gestión de un evento.

Se realiza una revisión de conceptos relevantes sobre seguridad informática, lo que permitió afirmar que la seguridad informática se enfoca a minimizar los riesgos existentes en el acceso y utilización mal intencionada de la información de los sistemas y aplicaciones. Es un tema que amerita la atención de la industria del desarrollo de aplicaciones. Diferentes metodologías, dentro de las que se incluye como guía fundamental el proyecto OWASP, corroboran la importancia conferida a la identificación de requisitos de seguridad y su seguimiento en el desarrollo del ciclo de vida de una aplicación.

Durante el estudio se logró definir los procedimientos para la identificación del estado actual sobre la gestión de eventos que pudieran terminar en incidentes de seguridad. Establecer un conjunto de procesos y patrones a seguir, lo

que permitió confeccionar un diseño que recoge desde el punto de vista conceptual la gestión de un incidente de seguridad, en su ciclo completo.

Otro aspecto conclusivo, y que no deja de tener importancia, trata sobre el trabajo sistemático con el hombre, puesto que al final, son los que están ejecutando las acciones detrás de las computadoras, muchos con mal intenciones premeditadas y otros, producto de la falta de conocimiento. En ambos casos la falta de concientización pudiera acarrear en males mayores.

No obstante, a medida que se incrementa el número de servicios y aplicaciones publicados en internet, la creciente interconexión de nuevos usuarios a las redes de datos, el surgimiento de nuevas tecnologías, y más importante la informatización de la sociedad, impone retos en cuanto a continuar explorando el mundo de la seguridad informática, no solo en aplicaciones web, sino como ámbito general. Exhortar a la nueva generación de especialistas, la constante capacitación y preparación en cuanto a la correcta utilización de la tecnología, así como la educación de los usuarios a ejercer buenas prácticas en la misma. No obstante, se entiende que ningún esquema por perfecto que parezca, nunca será totalmente seguro.

Referencias

1. *Pardo, M.R.V., et al., Comparación de tendencias tecnológicas en aplicaciones web. 2018.*
2. *Ikechukwu, U.I.J.G.J.o.C.S. and Technology, A Survey on Bandwidth Management Techniques Via the OSI Model Network and Application Layers. 2017.*
3. *Castillo, F.F.R., et al., Estado del arte: métricas de calidad para el desarrollo de aplicaciones web. 2017.* ***6****(4): p. 1-12.*
4. *Huanca Torres, F.A., Arquitectura para el desarrollo e implementación de servicios web. 2017.*
5. *Velasco, J.I.P., A.I.R. Ruiz, and H.A.P.J.T.I.y.A. Alvira, Arquitectura basada en microservicios para aplicaciones web. 2019.* ***7****(2): p. 12-20.*
6. *Brito, H.R.G., R.M. Perurena, and Y.Z. Véliz, CONTROLES DE SEGURIDAD PARA SISTEMAS DE GESTIÓN DE CONTENIDOS BASADOS EN SOFTWARE LIBRE SECURITY CONTROLS FOR CONTENT MANAGEMENT SYSTEMS BASED ON FREE SOFTWARE.*
7. *Comunicaciones, G.O.d.l.R.d.C.M.d., Resolución 128. Reglamento de Seguridad de las Tecnologías de La Información y la Comunicación. 2019.*
8. *Security., E.E.U.A.F.N.A.I., ENISA Threat Landscape 2015. 2016.*
9. *Security., E.E.U.A.F.N.A.I., ENISA Threat Landscape Report 2016. 2017.*
10. *Security., E.E.U.A.F.N.A.I., ENISA Threat Landscape Report 2017. 2018.*
11. *Security., E.E.U.A.F.N.A.I., ENISA Threat Landscape Report 2018. 2019.*

12. *Security., E.E.U.A.F.N.A.I., Web application attacks. 2020.*
13. *OWASP, O.W.A.S.P., Los diez riesgos más críticos en Aplicaciones Web. 2017.*
14. *OSRI., G.G.P., Administración de Incidentes de Seguridad Informática 2016.*
15. *Shirey, R., RFC2828: Internet security glossary. 2000, RFC Editor.*
16. *Brownlee, N. and E. Guttman, RFC2350: Expectations for computer security incident response. 1998, RFC Editor.*
17. *COMMERCE., N.F.-N.I.O.S.A.T.O.U.S.D.O., Minimum Security Requirements for Federal Information and Information Systems. 2006.*
18. *COMMERCE., N.S.-N.I.O.S.A.T.O.U.S.D.O., An Introduction to Information Security. 2017.*
19. *COMMERCE., N.S.-r.N.I.O.S.A.T.O.U.S.D.O., Security and Privacy Controls for Federal Information Systems and Organizations. 2020.*
20. *COMMERCE., N.S.-r.N.I.O.S.A.T.O.U.S.D.O., Computer Security Incident Handling Guide. 2012.*
21. *COMMERCE., N.S.-N.I.O.S.A.T.O.U.S.D.O., Guide for Security-Focused*

Configuration Management of Information Systems. 2011.
22. *COMMERCE., N.S.-N.I.O.S.A.T.O.U.S.D.O., Reports on Computer Systems Technology. 2011.*
23. *España, I.I.N.d.C.d., Procedimiento de gestión de ciberincidentes para el sector privado y la ciudadanía. 2018.*
24. *Group, O.I.S.S., Information Systems Security Assessment Framework. ISSAF. 2005.*
25. *OWASP., O.W.A.S.P., Testing Guide. 2014.*
26. *Amit, I.I., Penetration Testing Execution Standard. 2011.*
27. *COMMERCE., N.S.-N.I.O.S.A.T.O.U.S.D.O., Recommendations of the National Institute of Standards and Technology. 2008.*
28. *Harold A. Linstone, M.T., The Delphi Method.Techniques and Applications. 2002.*
29. *Deusto., U.d., EL MÉTODO DELPHI. 2004.*
30. *Fernández., R.L., expertos y prospectiva en la investigación pedagógica. 2016.*
31. *JULIO CABERO ALMENARA, J.B.O., EL COEFICIENTE DE COMPETENCIA EXPERTA. 2013.*
32. *Loor-Carvajal, G.I., El método Delphi. 2020.*
33. *Elena-Acebo, F.J., Aplicación del metodo delphi en el diseño de una investigación cuantitativa sobre el fenómeno FABLAB. 2018.*
34. *JOSEFA E. BLASCO MIRA, A.L., PADRÓNMENGUAL ANDRÉS, VALIDACIÓN MEDIANTE MÉTODO DELPHI DE UN CUESTIONARIO PARA CONOCER LAS EXPERIENCIAS E INTERÉS HACIA LAS ACTIVIDADES ACUÁTICAS CON ESPECIAL ATENCIÓN AL WINDSURF. 2010.*
35. *Dr.C. Idaris Gómez RaveloI, M.S.H.R.d.l.C.M., Software evaluación de expertos por el método Delphy para el pronóstico de la investigación agrícola. 2013.*