ANÁLISIS DE VULNERABILIDADES EN EL SISTEMA DE INVENTARIOS PHOENIX EN UNA IPS NIVEL 1

ANALYSIS OF VULNERABILITIES IN THE PHOENIX INVENTORY SYSTEM IN A LEVEL 1 IPS

Ing. Ricardo Alfonso Ruiz Cortes
raruizc@libertadores.edu.co
Fundación Universitaria Los Libertadores
Ing. Jhon Carlos Ruiz Cortes
jcruizc01@libertadores.edu.co
Fundación Universitaria Los Libertadores
Ing. Hector Manuel Herrera Herrera
hmherrerah@libertadores.edu.co

RESUMEN

Este artículo resume las técnicas usadas de *pentesting* en el sistema de inventarios *Phoenix* de una IPS de primer nivel, el cual es un desarrollo propio de la empresa basado en PHP y Mysql. Para esto se contemplaron 3 etapas: 1. El análisis e identificación del sistema de inventarios, se realizó utilizando una metodología de prueba de penetración, que incluyó una revisión de la documentación del sistema, entrevistas y visitas, para determinar el impacto que se pueda generar si se materializa una amenaza, está basado en la norma ISO 27001:2022, 2. Pentesting y pruebas de seguridad de la aplicación web. El estudio se llevó a cabo mediante una metodología de análisis de riesgos, que incluyó la identificación, evaluación y tratamiento de las vulnerabilidades identificadas. 3. Los

resultados del estudio mostraron que el sistema presentó una serie de vulnerabilidades que podrían ser explotadas por atacantes para obtener acceso a información confidencial o causar daños al sistema, posteriormente se genera una propuesta en la que se sugieren las mejores prácticas para mitigar estos riesgos. Se concluye que se deben aplicar acciones preventivas y correctivas por medio de políticas y procedimientos que deben ser verificados constantemente por los responsables de TI y la gerencia, realizando las actualizaciones pertinentes en cada una de ellas, aplicando los conceptos del PHVA y buenas prácticas de ITIL.

Palabras clave: análisis de vulnerabilidades, seguridad informática, identificación de riesgos, ISO 27001:2022, OWASP, escaneo de puertos.

ABSTRACT

This article summarizes the pentesting techniques used in the Phoenix inventory system of a first-level IPS, which is a company's own development based on PHP and Mysql. For this, 3 stages were contemplated: 1. The analysis and identification of the inventory system was carried out using a penetration testing methodology, which included a review of the system documentation, interviews and visits, to determine the impact that could be generated. If a threat materializes, it is based on the ISO 27001:2022 standard, 2. Pentesting and security testing of the web application. The study was carried out using a risk analysis methodology, which included the identification, evaluation and treatment of the identified vulnerabilities. 3. The results of the study showed that the system presented a series of vulnerabilities that could be exploited by attackers to obtain access to confidential information or cause damage to the system. Subsequently, a proposal is

generated in which best practices are suggested to mitigate these risks. . It is concluded that preventive and corrective actions must be applied through policies and procedures that must be constantly verified by those responsible for IT and management, making the pertinent updates in each of them, applying the concepts of the PHVA and good practices of ITIL.

Keywords: vulnerability analysis, computer security, risk identification, ISO 27001, OWASP, port scanning.

INTRODUCCIÓN

Las IPS son empresas que brindan servicios de salud a la población. En Colombia, las IPS están reguladas por el Ministerio de Salud y Protección Social y la Superintendencia Nacional de Salud (SNS). El SNS exige a las IPS que implementen medidas de seguridad para proteger la información de sus afiliados.

Los sistemas de inventarios son una parte importante de las operaciones de una IPS. Estos sistemas se utilizan para rastrear el inventario de medicamentos, suministros médicos y otros bienes. Las vulnerabilidades en los sistemas de inventarios pueden representar un riesgo para la seguridad de la información de los afiliados de la IPS.

de acuerdo a lo anterior en este artículo, se realizó un análisis de vulnerabilidades, basado en el sistema de inventarios PHOENIX en una IPS de nivel 1, en el cual se hace una propuesta para mitigar dichos hallazgos teniendo en cuenta que la información es actualmente uno de los recursos más importantes con el que cuentan las organizaciones, es por ello que se hace fundamental la aplicación de estrategias que

reduzcan el riesgo de ataques informáticos como lo son, la creación de políticas de seguridad de la información de acuerdo a las normas internacionales ISO 27001:2022, ley 1581 de 2012, decreto 1377 de 2013, COBIT, ITIL entre otras y crear metodologías que permitan la protección de los datos en las empresas prestadoras de salud.

FORMULACIÓN DEL PROBLEMA

¿Cuáles son las principales vulnerabilidades del sistema de inventario PHOENIX de la IPS nivel 1?

OBJETIVO GENERAL

Analizar las vulnerabilidades en el sistema de inventarios PHOENIX de una IPS de primer nivel. El análisis se realizó utilizando la metodología OWASP (*The Open Web Application Security Project*) que incluyó una revisión de la documentación del sistema basado en la norma ISO 27001:2022 y pruebas de seguridad de la aplicación web para determinar los controles adecuados garantizando la integridad, confidencialidad y disponibilidad de la información.

OBJETIVOS ESPECÍFICOS

1. Identificar las vulnerabilidades del sistema de información de inventario PHOENIX de la IPS nivel 1, por medio de escaneo de puertos en el servidor.
2. Describir vulnerabilidades en el sistema de información de inventarios de la IPS, realizando pruebas de penetración en el sistema.

3. Proponer la implementación de un modelo de análisis de vulnerabilidades y riesgos basado en la metodología OWASP del sistema de inventarios PHOENIX y los diferentes procesos que se llevan a cabo referente a mejores prácticas de desarrollo, cultura informática, procesos y procedimientos para la custodia de la información.

Alcance

El alcance de la propuesta es realizar el análisis de las vulnerabilidades como exploit, fallas, brechas de seguridad, puertos abiertos y errores de configuración en el sistema de inventarios PHOENIX.

REFERENTES TEÓRICOS

Antecedentes

Según informes generados por (John Maddison, 2023) VPE de Producto y CMO en Fortinet, El 80% de las organizaciones experimentan ciberataques que tienen a sus empleados como objetivo, la más reciente investigación de Fortinet en el primer semestre de 2023 indica que se han realizado más de 5.000 millones de intentos de ciberataques a infraestructuras públicas y privadas en Colombia. Las técnicas utilizadas para el ransomware son más sofisticadas y se dirigen principalmente a organizaciones dedicadas a la tecnología, la fabricación, el gobierno, las telecomunicaciones y la salud.

En su artículo, (Monsalve Pulido et al., 2014) Estudio y Gestión de Vulnerabilidades Informáticas para una Empresa Privada del Departamento de Boyacá (Colombia), analizaron diversos aspectos como la seguridad de acceso, la seguridad de los dispositivos, la gestión de contraseñas y el control de vulnerabilidades. Realizaron un inventario tecnológico inicial de la organización, identificaron y priorizaron las vulnerabilidades y aplicaron remedios manuales y automáticos. Basándose en estos datos, elaboraron un informe final con recomendaciones.

Por otro lado, (Niño Benitez, 2018) en su artículo *Requisitos de Seguridad para aplicaciones web* destacan algunos elementos para tener en cuenta como son: entrevistas con los responsables y directivos de la organización, los peligros que pueden afectar al sistema accidentalmente o que sean provocados y las medidas que se deben adoptar para prevenir y reducir los riesgos principalmente en aplicaciones web. Para mitigar las ciber amenazas y los riesgos, es esencial que las empresas y organizaciones apliquen medidas de seguridad que se ajusten a las normas ISO 27000, 27001, 27002 y metodologías como OWASP. En concreto, las aplicaciones basadas en web deben desarrollarse centrándose en la seguridad para minimizar las posibles vulnerabilidades. En última instancia, las organizaciones deben establecer políticas y procedimientos que permitan la implantación eficaz de un Sistema de Gestión de la Seguridad de la Información (SGSI) para reducir el riesgo de ciberataques.

Estado del Arte

La norma (ISO/CEI 27001:2022, 2022), Sistemas de Gestión de Seguridad de la Información, es un estándar internacional que proporciona un marco de trabajo para la gestión de la seguridad de la información (SSI). Esta norma es aplicable a cualquier organización, independientemente de su tamaño, sector o ubicación.

La importancia de la norma ISO 27001:2022 radica en los siguientes aspectos:

Protección de la información: La norma ISO 27001:2022 ayuda a las organizaciones a proteger su información confidencial, incluyendo datos personales, información comercial sensible y secretos empresariales.

Reducción de riesgos: La norma ISO 27001:2022 ayuda a las organizaciones a identificar y gestionar los riesgos de seguridad de la información a los que se enfrentan.

Mejora de la confianza: La certificación ISO 27001:2022 demuestra a los clientes, socios y otras partes interesadas que la organización está comprometida con la seguridad de la información.

Detectar vulnerabilidades en las redes, servidores y sitios web de empresas u organizaciones públicas y privadas es crucial para mitigar el riesgo de robo de información. Por lo tanto, la aplicación de metodologías de hacking ético resulta esencial. Según (Bakdash et al., 2018), la explotación no aleatoria de vulnerabilidades proporciona pruebas convergentes de la naturaleza sistemática de los ciberataques. Un pequeño número de estas tiende a constituir la mayoría de los exploits. Por ejemplo, las

violaciones de datos pueden clasificarse con una precisión del 90% utilizando dos tipos de riesgos observables externamente: a) sistemas internos mal configurados (por ejemplo, no cambiar los nombres de usuario y contraseñas por defecto) y b) tráfico saliente anómalo (por ejemplo, spam, escaneo de puertos). Otro enfoque utilizó los registros de monitorización de la red interna para identificar las probabilidades de que el malware utilice vectores vulnerables específicos (por ejemplo, configuración de la red, software sin parches y servicios concretos). Además de la vulnerabilidad, la previsibilidad puede observarse en el reducido número de direcciones IP o puntos de origen de los "atacantes", que representan la mayoría de los ciberataques.

El proceso de evaluar la seguridad de sitios o aplicaciones web realizando pruebas de penetración en servidores virtuales utilizando Kali Linux ha sido ampliamente adoptado (Campderrós Vilà, 2019). El sitio web de OWASP esboza una metodología de clasificación de riesgos que tiene en cuenta diversos factores para evaluar la probabilidad de que se produzca un riesgo este enfoque según (Jeff Williams, 2023) se basa en metodologías estándar y está personalizado para la seguridad de las aplicaciones en donde el Riesgo = Probabilidad * Impacto, para determinar la gravedad del riesgo se utiliza CVSS (first.org, n.d.)es un estándar publicado utilizado por organizaciones de todo el mundo, el sistema de puntuación de vulnerabilidad común por sus siglas en inglés (CVSS) proporciona una manera de capturar las características principales de una vulnerabilidad y producir una puntuación numérica que refleje su gravedad. Luego, la puntuación numérica se puede traducir en una representación cualitativa (como baja, media, alta y crítica) para ayudar a las organizaciones a evaluar y priorizar adecuadamente sus procesos de gestión de vulnerabilidades.

METODOLOGÍA

La metodología que se propone consiste en el análisis y detección de vulnerabilidades en el sistema de inventarios web de la IPS por medio de herramientas de código abierto, aplicando el enfoque cualitativo-descriptivo el cual permite extraer aquellas características primarias de las pruebas de penetración utilizadas en el sistema de inventarios.

Ilustración 1 Metodología
Fuente: elaboración propia

- **Análisis e identificación del sistema de inventario PHOENIX**

En esta primera fase se realiza una inspección física en el servidor del sistema de inventarios, incluyendo la verificación de la configuración del servidor, la instalación de software y los procedimientos de seguridad.

Las técnicas de análisis de vulnerabilidades que se aplicaron fueron las siguientes:

1. Análisis de seguridad lógica
2. Análisis de seguridad de la información

- **Pruebas de seguridad**

Durante la segunda fase se realizaron pruebas de seguridad al sistema de inventarios, utilizando herramientas de software libre como Kali Linux y ZAP aplicando técnicas de evaluación de vulnerabilidades.

- **Presentación de los resultados**

Para la última fase una vez identificados todos los riesgos potenciales, se documentan los resultados obtenidos, junto con las conclusiones del trabajo realizado y finalmente se genera la propuesta teniendo en cuenta que cada una de las etapas desarrolladas en este artículo, se ajusta a las normas y estándares internacionales vigentes basado en la norma ISO 27001:2022 y la metodología OWASP.

ANALISIS Y RESULTADOS

El análisis identificó una serie de vulnerabilidades en el sistema de inventarios PHOENIX, algunas de las cuales eran críticas. Las vulnerabilidades más comunes se encontraban en las áreas de seguridad lógica y seguridad de la información.

Fase 1 Análisis e identificación del sistema de inventario PHOENIX

La fase 1 se desarrolló de acuerdo con el cronograma, los permisos otorgados por la IPS y el jefe de sistemas de la regional, se realizaron 5 visitas en un mes con una duración de 2 horas cada visita, donde se permitió el ingreso al área que aloja el servidor de la aplicación PHOENIX y se asignó la conexión a la red local por medio de una ip estática, haciendo un reconocimiento general del sistema de inventarios y realizando entrevistas a los responsables del área en la cual se tomaron datos pertinentes a la metodología y procesos que aplica el área de TI para realizar análisis de vulnerabilidades y la metodología utilizada actualmente, para la mitigación de riesgos en el sistema. El siguiente diagrama de Gantt muestra el plan de trabajo realizado.

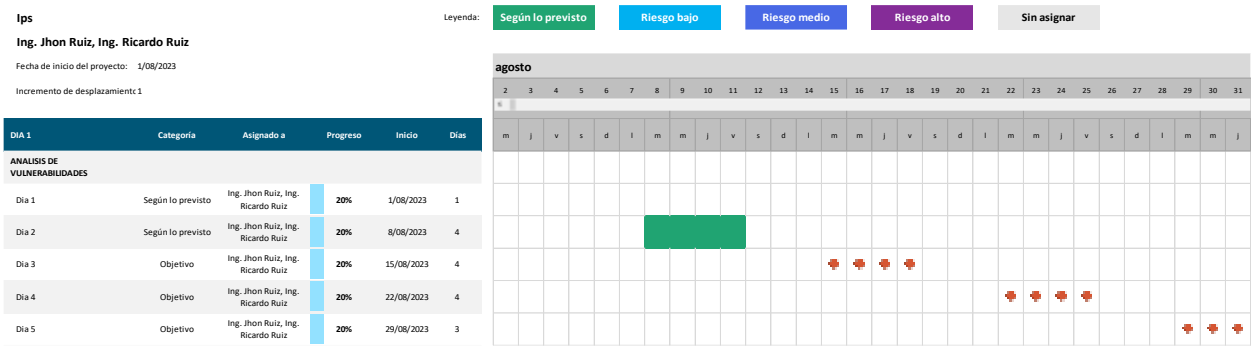


Ilustración 2 Tabla Diagrama de Gantt
Fuente: elaboración propia

De acuerdo con los datos obtenidos en esta primera fase se identificaron las siguientes vulnerabilidades en el sistema de inventarios:

Seguridad lógica:

- Falta de actualización de los sistemas operativos y el software.

Seguridad de la información:

- Falta de políticas y procedimientos de seguridad de la información.
- Falta de capacitación del personal en seguridad de la información.

Infraestructura Actual

Sistema Operativo	protocolos/servicios expuestos	Red
Windows server 2012 r2	Apache httpd 2.4.17 - OpenSSL/1.0.2d - PHP 5.6.21	Interna

Tabla 1 Infraestructura actual
Fuente: elaboración propia

Estado actual del sistema de inventario PHOENIX

Tabla 1. Análisis de los controles anexo A basados en la norma ISO/IEC 27001:2022

Sección	Control de seguridad de la información	Status
A5	**Controles organizacionales**	
A.5.7	Inteligencia de amenazas	Inexistente
A.5.8	Seguridad de la información en la gestión de proyectos	Inexistente
A.5.9	Inventario de activos de información y otros asociados a la misma	Inexistente
A.5.12	Clasificación de la información	Inexistente
A.5.15	Control de Acceso	Inexistente
A.5.18	Derechos de acceso	Inexistente
A.5.24	Planeamiento y preparación de la gestión de incidentes de seguridad de la información	Inexistente
A.5.25	Evaluación y decisión en los eventos de seguridad de la información	Inexistente
A.5.26	Respuesta a los incidentes de seguridad de la información	Inexistente
A.5.27	Aprendizaje sobre los incidentes de seguridad de la información	Inexistente
A.5.28	Recolección de evidencia	Inexistente
A.5.30	Preparación de las TIC para la continuidad de negocio	Inexistente

A.5.33	Protección de registros	Inexistente
A.5.34	Privacidad y protección de la PII (Información Identificable Personal)	Inexistente
A.5.37	Procedimientos operacionales documentados	Inexistente
A6		
A.6.2	Términos y condiciones de empleo	Inexistente
A7		
A.7.1	Perímetros de seguridad física	Inexistente
A8		
A.8.3	Restricción de acceso a la información	Inexistente
A.8.5	Autenticación segura	Inexistente
A.8.24	Uso de criptografía	Inexistente
A.8.25	Desarrollo seguro del ciclo de vida	Inexistente
A.8.26	Requerimientos de seguridad en aplicaciones	Inexistente
A.8.27	Principios de arquitectura de sistemas e ingeniería seguras	Inexistente
A.8.28	Generación de código seguro	Inexistente
A.8.29	Prueba segura en el desarrollo y aceptación	Inexistente
A.8.31	Separación de entornos de desarrollo, prueba y producción	Inexistente
A.8.32	Gestión de cambios	Inexistente
A.8.33	Información de prueba	Inexistente
A.8.34	Protección de sistemas de información durante pruebas de auditoría	Inexistente

Fuente: (iso27001security, 2023)

Tabla 2. Métricas

Status	Significado	Proporción de requisitos del SGSI	Proporción de controles de seguridad de la información
? Desconocido	No ha sido siquiera revisado aún	**0%**	**69%**

Inexistente	Ausencia completa de una política, procedimiento, control, etc legibles	**100%**	**31%**
Inicial	El desarrollo apenas ha comenzado y requerirá un trabajo significativo para satisfacer los requisitos	**0%**	**0%**
Limitado	Progresando bien pero no completado aún	**0%**	**0%**
Definido	El desarrollo está más o menos completo aunque con ausencia de detalles y/o no está aún implementado, en cumplimiento vigente ni activamente avalado por la alta dirección.	**0%**	**0%**
Gestionado	El desarrollo está completo, el proceso / control ha sido implementado y recientemente comenzó a operar	**0%**	**0%**
Optimizado	El requisito está plenamente conforme, está plenamente operativo como se espera, está siendo activamente supervisado y mejorado, y hay evidencia sustancial para demostrar todo lo antedicho a los auditores	**0%**	**0%**
No Aplica	TODOS los requerimientos en el cuerpo principal de la norma ISO/IEC 27001 son obligatorios SI su SGSI va a ser certificado. Caso contrario, la gerencia a cargo, puede ignorarlos	**0%**	**0%**
	Total	100%	100%

Fuente: (iso27001security, 2023)

Fase 2 pruebas de seguridad pentesting

En la segunda fase se realizaron pruebas en Kali Linux con nmap, cuyo resultado evidenció las versiones del sistema operativo, apache httpd, openssl y PHP respectivamente.

Posteriormente Se realizó un escaneo con la herramienta zap 2.14.0 para verificar la url de la IPS, según el top 10 de OWASP.

Ilustración 3 Identificación de puertos, servicios y sistema operativo
Fuente: elaboración propia

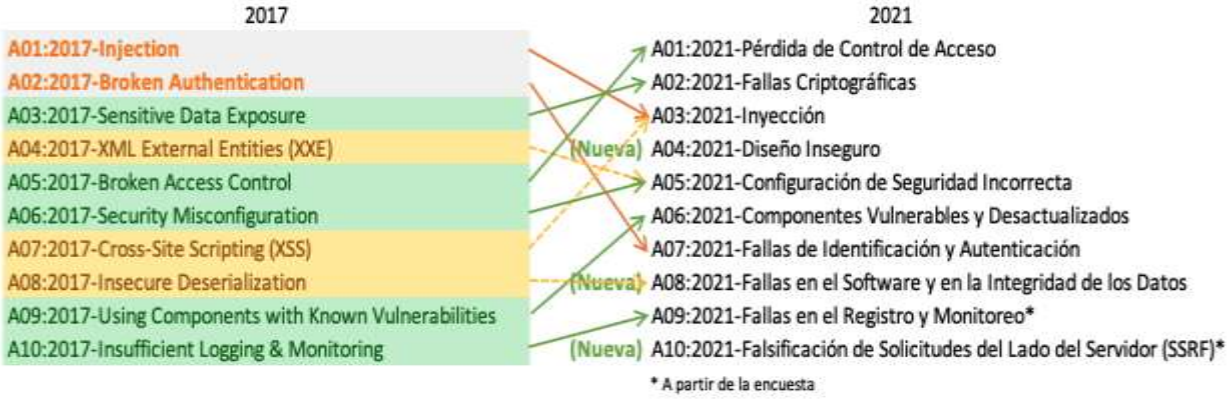


Ilustración 4 OWASP Top 10:2021
Fuente:(owasp.org, 2021)

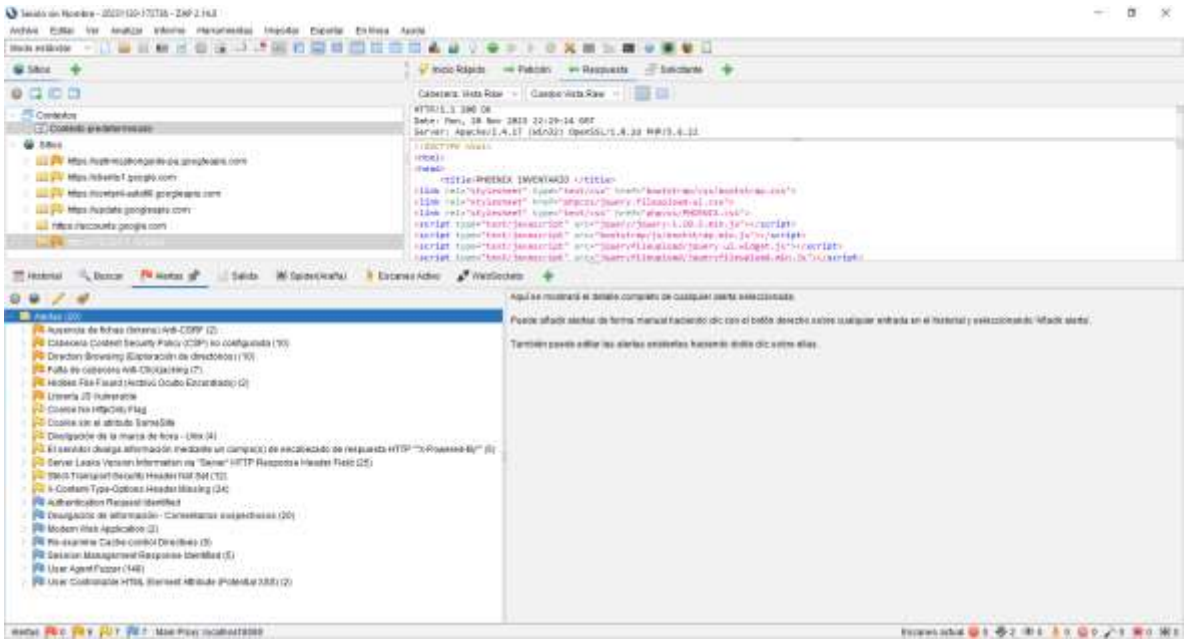


Ilustración 5 Escaneo de la url aplicación *PHOENIX* con zap 2.14.0
Fuente: elaboración propia

Fase 3 presentación de los resultados

Tabla 3. Resultados obtenidos del escaneo de puertos nmap

PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
443/tcp	open	ssl/http	Apache httpd 2.4.17 ((win32) openSSL/1.0.2d PHP/5.6.21)
445/tcp	open	Microsoft-ds	Microsoft Windows Server 2008 R2-2012 microsoft-ds
3306/tcp	open	mysql	MySQL 5.5.5-10.1.13-MariaDB
3389/tcp	open	ssl/ms-wbt-server?	
8080/tcp	open	http	Apache httpd 2.4.17 ((win32) openSSL/1.0.2d PHP/5.6.21)
49152/tcp	open	msrpc	Microsoft Windows RPC
49153/tcp	open	msrpc	Microsoft Windows RPC
49154/tcp	open	msrpc	Microsoft Windows RPC
49155/tcp	open	msrpc	Microsoft Windows RPC
49156/tcp	open	msrpc	Microsoft Windows RPC

Fuente: elaboración propia

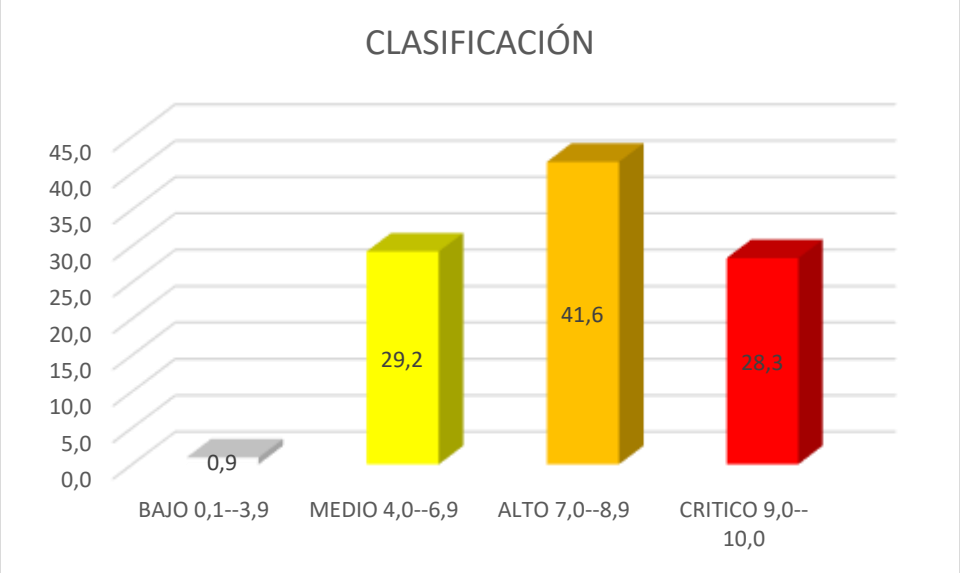
El resultado nos expuso las vulnerabilidades por cada una de las versiones de software instaladas en el servidor, por ejemplo y según la escala CVSS las más críticas así:

En la capa de transporte del protocolo openSSL y la capa de aplicación del protocolo apache http del lenguaje de programación PHP, de acuerdo con la escala CVSS Scores un total de 219 Vulnerabilidades clasificadas de la siguiente manera:

Tabla 4. Matriz de impacto vulnerabilidades según escala CVSS Scores.

CLASIFICACION	PUNTAJE	NUMERO DE VULNERABILIDADES	PORCENTAJE
BAJO	BAJO 0,1--3,9	2	0,9
MEDIO	MEDIO 4,0--6,9	64	29,2
ALTO	ALTO 7,0--8,9	91	41,6
CRITICO	CRITICO 9,0--10,0	62	28,3
	TOTALES	219	100

Fuente: elaboración propia



Grafica 1 Clasificación de vulnerabilidades escala CVSS Scores
Fuente: elaboración propia

Las principales vulnerabilidades del sistema de inventarios PHOENIX son las clasificadas en alto y critico las cuales suman 153, estas deben corregirse de forma

inmediata. Las vulnerabilidades de clasificación alto deben ser revisadas y la corrección se debe hacer siempre que sea posible.

A continuación, se muestran los resultados de acuerdo con el protocolo analizado.

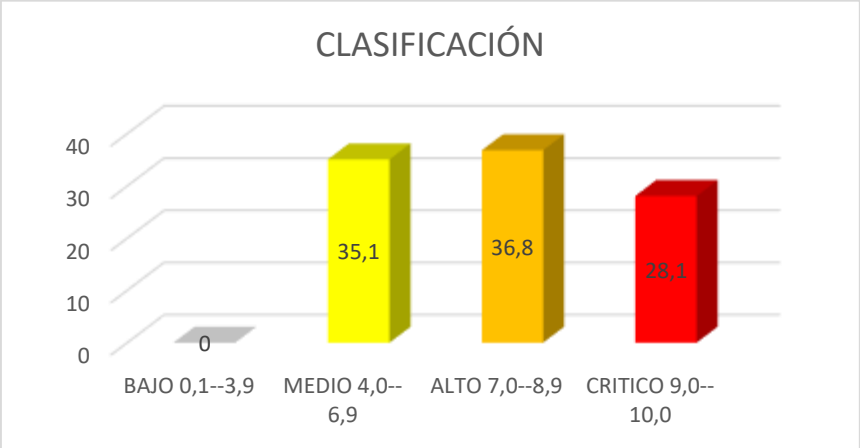
APACHE http server 2.4.17

Se hallaron 57 vulnerabilidades las cuales están identificadas según su número y clasificación.

Tabla 5. Matriz de impacto vulnerabilidades Apache server 2.4.17

CLASIFICACION	PUNTAJE	NUMERO DE VULNERABILIDADES	PORCENTAJE
BAJO	BAJO 0,1--3,9	0	0
MEDIO	MEDIO 4,0--6,9	20	35,1
ALTO	ALTO 7,0--8,9	21	36,8
CRITICO	CRITICO 9,0--10,0	16	28,1
	TOTALES	57	100

Fuente: elaboración propia



Grafica 2 Clasificación de vulnerabilidades Apache Server 2.4.17
Fuente: elaboración propia

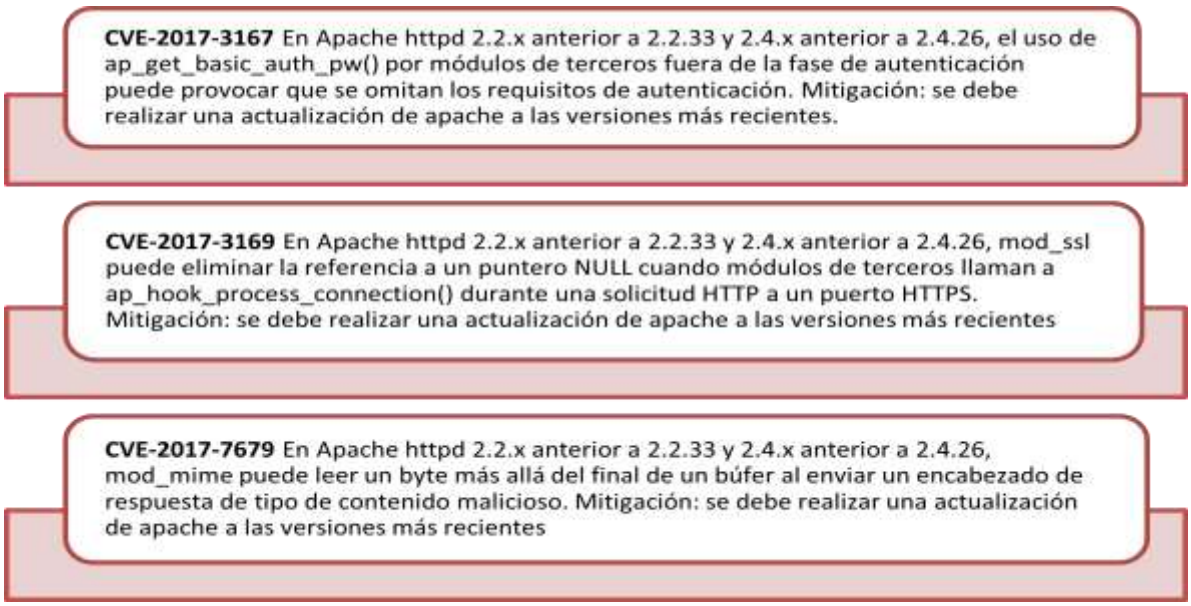


Ilustración 6 Apache httpd 2.4.17, puntaje de 9,8 se muestran 3 resultados con severidad Critica
Fuente: elaboración propia

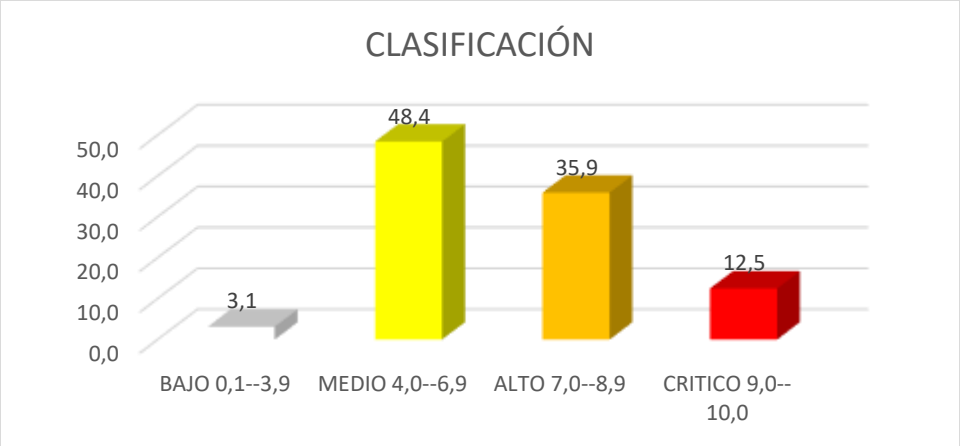
OPENSSL 1.0.2d

Se hallaron 64 vulnerabilidades las cuales están identificadas según su número y clasificación.

Tabla 6. Matriz de impacto vulnerabilidades OPENSSL 1.0.2d

CLASIFICACION	PUNTAJE	NUMERO DE VULNERABILIDADES	PORCENTAJE
BAJO	BAJO 0,1—3,9	2	3,125
MEDIO	MEDIO 4,0—6,9	31	48,4
ALTO	ALTO 7,0—8,9	23	35,9
CRITICO	CRITICO 9,0—10,0	8	12,5
	TOTALES	64	100

Fuente: elaboración propia



Grafica 3 Clasificación de vulnerabilidades OPENSSL 1.0.2d
Fuente: elaboración propia

CVE-2016-0705 Doble vulnerabilidad gratuita en la función dsa_priv_decode en crypto/dsa/dsa_ameth.c en OpenSSL 1.0.1 anterior a 1.0.1s y 1.0.2 anterior a 1.0.2g permite a atacantes remotos provocar una denegación de servicio (corrupción de memoria) o posiblemente tener otro impacto no especificado a través de una clave privada DSA con formato incorrecto. Mitigación: se debe realizar una actualización de Open SSL a la versión más reciente.

CVE-2016-0799 La función fmtstr en crypto/bio/b_print.c en OpenSSL 1.0.1 anterior a 1.0.1s y 1.0.2 anterior a 1.0.2g calcula incorrectamente longitudes de cadena, lo que permite a atacantes remotos provocar una denegación de servicio (desbordamiento y fuera de servicio). límites leídos) o posiblemente tener otro impacto no especificado a través de una cadena larga, como lo demuestra una gran cantidad de datos ASN.1, una vulnerabilidad diferente a CVE-2016-2842. Mitigación: se debe realizar una actualización de Open SSL a la versión más reciente.

CVE-2016-2842 La función doapr_outch en crypto/bio/b_print.c en OpenSSL 1.0.1 anterior a 1.0.1s y 1.0.2 anterior a 1.0.2g no verifica que una determinada asignación de memoria tenga éxito, lo que permite a atacantes remotos provocar una denegación de servicio (fuera de -de límites de escritura o consumo de memoria) o posiblemente tener otro impacto no especificado a través de una cadena larga, como lo demuestra una gran cantidad de datos ASN.1, una vulnerabilidad diferente a CVE-2016-0799. Mitigación: se debe realizar una actualización de Open SSL a la versión más reciente.

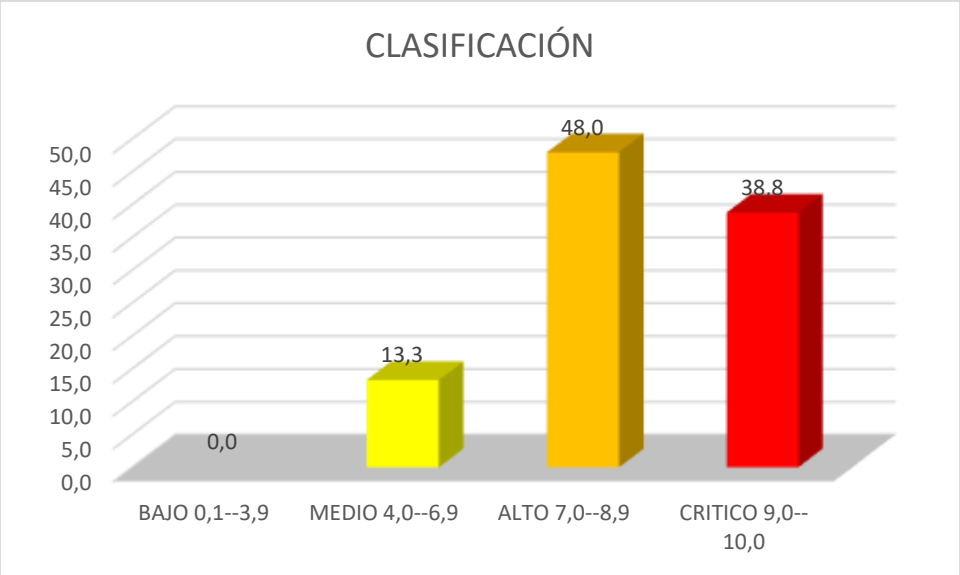
Ilustración 7 OpenSSL/1.0.2d, puntaje de 10 se muestran 3 resultados con severidad Critica
Fuente: elaboración propia

PHP 5.6.21

Tabla 7. Matriz de impacto vulnerabilidades PHP 5.6.21

CLASIFICACION	PUNTAJE	NUMERO DE VULNERABILIDADES	PORCENTAJE
BAJO	BAJO 0,1--3,9	0	0
MEDIO	MEDIO 4,0--6,9	13	13,3
ALTO	ALTO 7,0--8,9	47	48,0
CRITICO	CRITICO 9,0--10,0	38	38,8
	TOTALES	98	100

Fuente: elaboración propia



Grafica 4 Clasificación de vulnerabilidades PHP 5.6.21
Fuente: elaboración propia

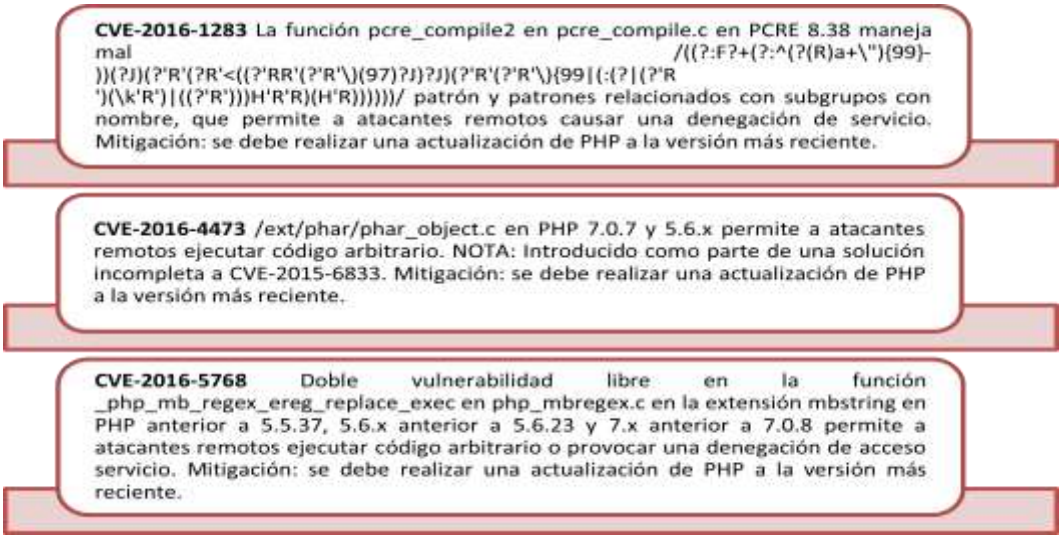


Ilustración 8 PHP 5.6.21, puntaje de 9,8 se muestran 3 resultados con severidad Critica
Fuente: elaboración propia

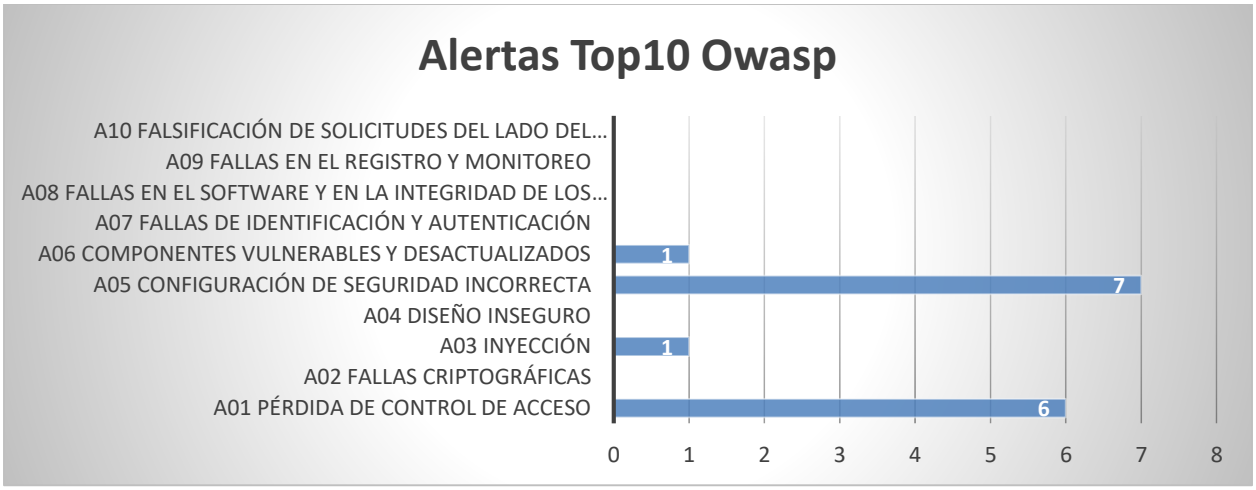
Tabla 8. Resultados OWASP Top 10:2021

TOP 10 OWASP	Numero de ALERTAS	DESCRIPCION
OWASP_2021_A01	**6**	**A01:2021 - Pérdida de Control de Acceso** sube de la quinta posición a la categoría con el mayor riesgo en seguridad de aplicaciones web; los datos proporcionados indican que, en promedio, el 3,81% de las aplicaciones probadas tenían una o más Common Weakness Enumerations (CWEs) con más de 318.000 ocurrencias de CWEs en esta categoría de riesgo. Las 34 CWEs relacionadas con la Pérdida de Control de Acceso tuvieron más apariciones en las aplicaciones que cualquier otra categoría.
OWASP_2021_A03	**1**	**A03:2021 - Inyección** sube una posición ubicándose en la segunda, antes conocida como A3:2017-Exposición de Datos Sensibles, que era más una característica que una causa raíz. El nuevo nombre se centra en las fallas relacionadas con la criptografía, como se ha hecho implícitamente antes. Esta categoría frecuentemente conlleva a la exposición de datos confidenciales o al compromiso del sistema.

OWASP_2021_A05	**7**	**A05:2021 - Configuración de Seguridad Incorrecta** asciende desde la sexta posición en la edición anterior; el 90% de las aplicaciones se probaron para detectar algún tipo de configuración incorrecta, con una tasa de incidencia promedio del 4,5% y más de 208.000 casos de CWEs relacionadas con esta categoría de riesgo. Con mayor presencia de software altamente configurable, no es sorprendente ver qué esta categoría ascendiera. El A4:2017-Entidades Externas XML(XXE), ahora en esta edición, forma parte de esta categoría de riesgo.
OWASP_2021_A06	**1**	**A06:2021 - Componentes Vulnerables y Desactualizados** antes denominado como Uso de Componentes con Vulnerabilidades Conocidas, ocupa el segundo lugar en el Top 10 de la encuesta a la comunidad, pero también tuvo datos suficientes para estar en el Top 10 a través del análisis de datos. Esta categoría asciende desde la novena posición en la edición 2017 y es un problema conocido que cuesta probar y evaluar el riesgo. Es la única categoría que no tiene ninguna CVE relacionada con las CWEs incluidas, por lo que una vulnerabilidad predeterminada y con ponderaciones de impacto de 5,0 son consideradas en sus puntajes.

Fuente: elaboración propia

Grafica 4 Clasificación de alertas por riesgo sistema *PHOENIX*
Fuente: elaboración propia



Grafica 5 Alertas encontradas OWASP Top 10:2021 sistema *PHOENIX*
Fuente: elaboración propia

Ciclo propuesto de mejora

Se propuso aplicar el ciclo PHVA ya que es una herramienta efectiva para mejorar los procesos y alcanzar los objetivos deseados. A través de las etapas de planificar, hacer, verificar y actuar, la IPS puede identificar áreas de mejora, implementar cambios efectivos y mantener la excelencia en sus operaciones. Además, el análisis de vulnerabilidades es una herramienta valiosa para identificar y abordar las debilidades en los procesos actuales.

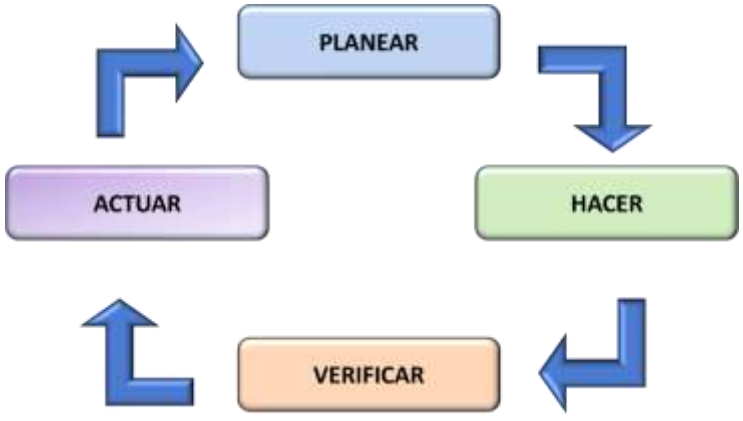


Ilustración 9 Ciclo propuesto PHVA
Fuente: elaboración propia

En el contexto del análisis de vulnerabilidades, el ciclo PHVA se puede utilizar para implementar un programa de gestión de riesgos de seguridad de la información (SGSI) que cumpla con las normas ISO/IEC 27001:2022 e ISO/IEC 27005:2018.

Planear: En la fase de planificación, es importante definir claramente los objetivos y establecer un plan detallado para alcanzarlos. Esto implica identificar los recursos necesarios, asignar responsabilidades y establecer plazos realistas. Además, es fundamental considerar cualquier riesgo potencial y desarrollar estrategias para mitigarlos.

En el caso de la IPS NIVEL 1, los objetivos de la detección de vulnerabilidades pueden ser:

- Identificar y mitigar las vulnerabilidades de los sistemas de información, para proteger la confidencialidad, integridad y disponibilidad de los datos.
- Cumplir con los requisitos de las normas ISO/IEC 27001:2022 e ISO/IEC 27005:2018.

Los recursos necesarios para la detección de vulnerabilidades pueden incluir:

- Personal capacitado en seguridad de la información.
- Herramientas de evaluación de vulnerabilidades.
- Acceso a información sobre vulnerabilidades.

El cronograma de trabajo debe definir las fechas de inicio y finalización de cada actividad, así como los responsables de cada una. Los activos de información que se deben proteger en el sistema de inventario PHOENIX incluyen:

- Datos de pacientes, como nombres, fechas de nacimiento, números de identificación, historial médico, etc.
- Datos de operaciones, como registros de inventario.

Los riesgos a los que están expuestos estos activos de información incluyen:

- Acceso no autorizado
- Modificación no autorizada
- Destrucción no autorizada
- Revelación no autorizada

Hacer: Una vez que se ha establecido un plan sólido, es hora de ponerlo en acción. La fase de hacer implica implementar el plan y llevar a cabo las actividades definidas en la etapa de planificación. Es importante asegurarse de que todos los recursos necesarios estén disponibles y que el personal esté debidamente capacitado para llevar a cabo las tareas asignadas. Es fundamental mantener una comunicación clara y abierta con todos los miembros del equipo. Esto garantizará que todos estén al tanto de sus responsabilidades y que cualquier problema o desviación se aborde de inmediato. Además, es importante monitorear de cerca el progreso y realizar ajustes si es necesario.

En este paso, se implementan las actividades planificadas.

Las actividades específicas de detección de vulnerabilidades pueden incluir:

- Análisis de vulnerabilidades internas.
- Análisis de vulnerabilidades externas.
- Monitoreo continuo de vulnerabilidades.

las medidas de control que se pueden implementar incluyen:

- Controles de acceso, como contraseñas seguras, dos factores de autenticación, etc.
- Controles de cifrado, para proteger los datos confidenciales
- Controles de auditoría, para registrar las actividades de los usuarios

Verificar: Una vez que se ha completado la fase de hacer, es hora de evaluar los resultados. La fase de verificación implica comparar los resultados obtenidos con los objetivos establecidos en la etapa de planificación, recopilar y analizar datos relevantes para determinar si se han alcanzado los resultados deseados. Es importante ser objetivo y honesto al evaluar los resultados. Si se han alcanzado los objetivos, se pueden identificar las mejores prácticas y replicarlas en futuros proyectos. Sin embargo, si los resultados no cumplen con las expectativas, es fundamental identificar las causas y tomar medidas correctivas.

En este paso, se evalúan los resultados de las actividades realizadas. La evaluación de la detección de vulnerabilidades puede incluir:

- Análisis de los resultados de las evaluaciones de vulnerabilidades.
- Seguimiento de las vulnerabilidades identificadas.

Actuar: En esta etapa, se toman medidas basadas en los resultados obtenidos en la fase de verificación. Si los resultados son positivos, se pueden implementar acciones para mantener y mejorar los procesos existentes. Por otro lado, si los resultados no son satisfactorios, se deben tomar medidas correctivas para abordar las deficiencias identificadas.

Las acciones específicas que se pueden tomar para mejorar la detección de vulnerabilidades pueden incluir:

- Actualización de las herramientas de evaluación de vulnerabilidades.
- Capacitación adicional del personal en seguridad de la información.
- Implementación de nuevas medidas de seguridad.

Repetir: El ciclo PHVA es un ciclo continuo, por lo que se debe repetir periódicamente para garantizar que el sistema de inventario siga siendo seguro.

En el caso específico de la IPS NIVEL 1, se deben considerar los siguientes aspectos adicionales en el análisis de vulnerabilidades:

- La protección de la privacidad: Los datos de los pacientes son datos personales sensibles, por lo que se deben tomar medidas especiales para proteger su privacidad.
- La disponibilidad del sistema: El sistema de inventario debe estar disponible para los usuarios autorizados en todo momento.

- La integridad de los datos: Los datos del sistema de inventario deben estar protegidos de la manipulación o destrucción.

Propuesta: Se propone a la IPS NIVEL 1, implementar un sistema de gestión de seguridad de la información SGSI, basado en las normas ISO 27001:2022 e ISO 27005:2018 con el apoyo del proyecto OWASP para el desarrollo de software seguro, además de un plan de recuperación de desastres DRP. La implementación de la metodología OWASP es un proceso que requiere de la participación de todos los niveles de la organización, desde la alta dirección hasta los desarrolladores y usuarios. El objetivo es establecer una cultura de seguridad en toda la organización y reducir el riesgo de ataques a las aplicaciones web, esta implementación puede dividirse en las siguientes etapas:

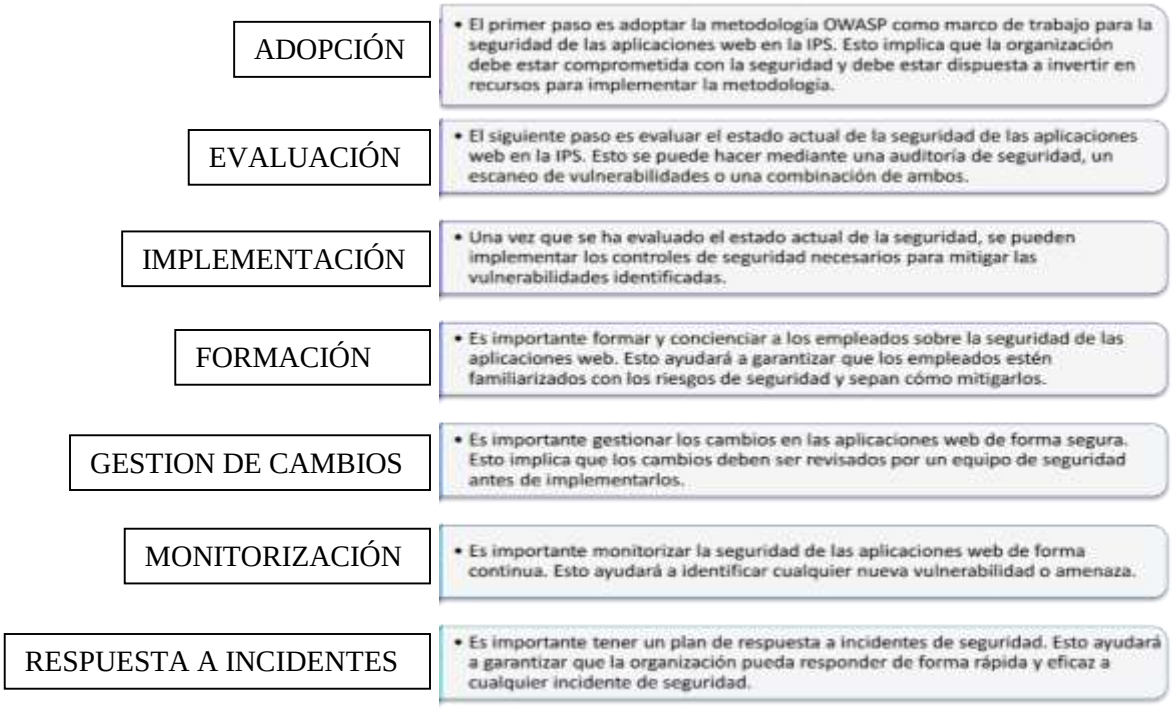


Ilustración 10 etapas propuestas para implementación del SGSI metodología OWASP
Fuente: elaboración propia

En el caso de la IPS, la implementación de la metodología OWASP puede ser particularmente importante para proteger la información personal de los pacientes. Las aplicaciones web que utilizan estos sistemas de información deben ser especialmente seguras para evitar que se vea comprometida.

A continuación, se presentan algunos ejemplos específicos de cómo se puede implementar la metodología OWASP en la IPS NIVEL 1:

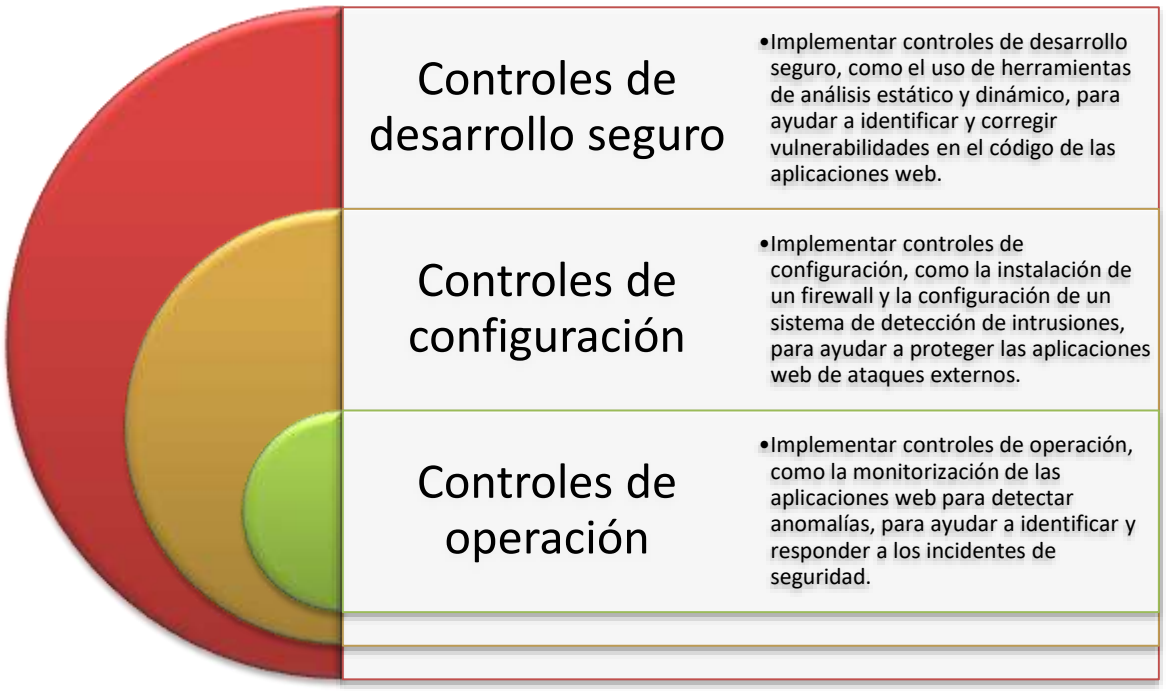


Ilustración 11 implementación propuesta de controles de seguridad aplicando la metodología OWASP
Fuente: elaboración propia

El análisis de vulnerabilidades debe realizarse de acuerdo con el siguiente procedimiento:

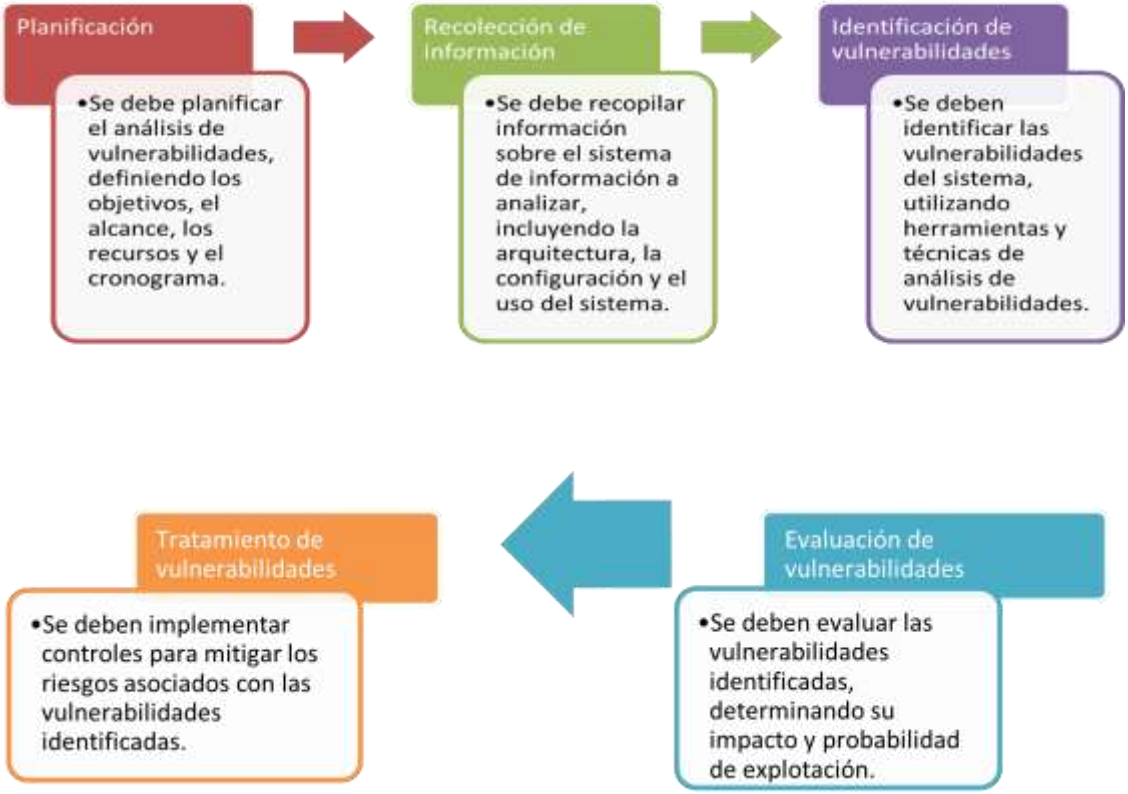


Ilustración 12 procedimiento sugerido para análisis de vulnerabilidades
Fuente: elaboración propia

Recomendaciones

Realizar el análisis con regularidad: Debe realizarse de forma periódica, para identificar nuevas vulnerabilidades y evaluar las existentes.

Utilizar herramientas y técnicas de alta calidad: Las herramientas y técnicas de análisis de vulnerabilidades deben ser de alta calidad, para garantizar la identificación de todas las relevantes.

Involucrar a expertos en seguridad de la información: Debe ser realizado por expertos en seguridad de la información, para garantizar que se realice de forma adecuada.

CONCLUSIONES

El análisis de vulnerabilidades es una parte importante en la gestión de la seguridad de los sistemas informáticos, permitiendo identificar y mitigar los riesgos de seguridad que pueden afectar a la integridad, disponibilidad y confidencialidad de los datos. En este artículo se ha presentado un análisis de vulnerabilidades en el sistema de inventarios PHOENIX de una IPS NIVEL 1, se llevó a cabo utilizando una combinación de métodos manuales y automatizados.

Los resultados obtenidos muestran que el sistema de inventarios presentaba una serie de vulnerabilidades, algunas de las cuales eran críticas. Las más comunes se encontraban en las áreas de seguridad lógica y seguridad de la información.

Las buenas prácticas establecidas en esta propuesta permiten realizar un análisis de vulnerabilidades eficaz y eficiente, que contribuya a proteger el sistema de inventario PHOENIX de las IPS NIVEL 1 y establecer políticas y procedimientos para la protección de los datos.

Implementar la metodología OWASP en la IPS es una tarea compleja, pero es esencial para proteger los datos y recursos sensibles de la organización. Con una planificación cuidadosa y la participación de todos los niveles de la organización, es posible lograrlo de forma exitosa.

REFERENCIAS BIBLIOGRÁFICAS

Bakdash, J. Z., Hutchinson, S., Zaroukian, E. G., Marusich, L. R., Thirumuruganathan, S., Sample, C., Hoffman, B., & Das, G. (2018). Malware in the future? Forecasting of analyst detection of cyber events. *Journal of Cybersecurity*, *4*(1), tyy007. https://doi.org/10.1093/cybsec/tyy007

Campderrós Vilà, J. (2019, May). *Ataques y vulnerabilidades web*. Http://Hdl.Handle.Net/2445/143419.

first.org. (n.d.). *https://www.first.org/cvss/*.

iso27001security. (2023, November 14). *iso27001security*. Https://Www.Iso27001security.Com/ISO27k_SGSI_6.1_SoA_2022_Espanol_Rev03.Xlsx.

ISO/CEI 27001:2022. (2022, October). *ISO/CEI 27001:2022*. Https://Www.Iso.Org/Standard/27001.

Jeff Williams. (2023, October 15). *Metodología de calificación de riesgos de OWASP*. Https://Owasp.Org/Www-Community/OWASP_Risk_Rating_Methodology.

John Maddison. (2023, June 12). *El 80% de las organizaciones experimentan ciberataques que tienen a sus empleados como objetivo, según la más reciente investigación de Fortinet*. Https://Www.Fortinet.Com/Lat/Corporate/about-Us/Newsroom/Press-Releases/2023/Fortinet-Research-Finds-over-80-Perfect-of-Organizations-Experience-Cyber-Attacks-That-Target-Employees.

Monsalve Pulido, J. A., Aponte Novoa, F. A., & Chaves Tamayo, D. fernando. (2014). Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá (Colombia). *Revista Facultad de Ingeniería (Fac. Ing.)*, *23*, 65–72.

Niño Benitez, Y. (2018). Requisitos de Seguridad para aplicaciones web Security Requirements for web applications. *No. Especial UCIENCIA*, *12*, 205–221. http://rcci.uci.cuhttp://rcci.uci.cu

owasp.org. (2021). *OWASP Top 10:2021*. Https://Owasp.Org/Top10/Es/#como-Se-Utilizan-Los-Datos-Para-Seleccionar-Las-Categorias.