# ANALISIS DEL SISTEMA DE SEGURIDAD DE LA INFORMACION EN LA EPS-INDIGENA PIJAOS SALUD SEDE IBAGUE PARA EL CONTROL DE VULNERABILIDADES UTILIZANDO HACKING ETICO

WALTER KELIN PORRAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUE
2022

# ANALISIS DEL SISTEMA DE SEGURIDAD DE LA INFORMACION EN LA EPS-INDIGENA PIJAOS SALUD SEDE IBAGUE PARA EL CONTROL DE VULNERABILIDADES UTILIZANDO HACKING ETICO

WALTER KELIN PORRAS

Proyecto de Grado – Proyecto Aplicado presentado para optar por el título de ESPECIALISTA EN SEGURIDAD INFORMATICA

Nombre
JOEL CARROLL VARGAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUE
2022

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

## DEDICATORIA

Con amor dedico éste trabajo a mi hija, que con su carisma y comprensión me acompañó en cada etapa vivida, colaborándome de manera indirecta, minimizando mis preocupaciones de madre, también lo dedico a mi mamá que con su apoyo, consagración y paciencia disminuyo mis tareas en el hogar permitiéndome una entrega tranquila en el estudio y trabajo.

## AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado a cada uno de los tutores y asesores que me acompañaron en el proceso les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

## CONTENIDO

pág.


*INTRODUCCIÓN* ..... *15*

*1. DEFINICIÓN DEL PROBLEMA* ..... *16*

**1.1 ANTECEDENTES DEL PROBLEMA** ..... **16**

**1.2 FORMULACIÓN DEL PROBLEMA** ..... **17**

*2 JUSTIFICACIÓN* ..... *18*

*3 OBJETIVOS* ..... *20*

**3.1 OBJETIVOS GENERAL** ..... **20**

**3.2 OBJETIVOS ESPECÍFICOS** ..... **20**

*4 MARCO REFERENCIAL* ..... *21*

**4.1 MARCO TEÓRICO** ..... **21**

4.1.1 Referente Bibliográfico ..... 21
4.1.2 Importancia del hacking ético en una organización ..... 21
4.1.3 Amenazas informáticas ..... 21
4.1.4 Beneficios del Hacking ético ..... 22
4.1.5 Pruebas de penetración de Caja blanca ..... 22
4.1.6 Pruebas de penetración de Caja negra ..... 22
4.1.7 Pruebas de penetración de Caja gris ..... 23

**4.2 MARCO CONCEPTUAL** ..... **23**

**4.3 MARCO HISTÓRICO** ..... **25**

**4.4 ANTECEDENTES O ESTADO ACTUAL** ..... **25**

Estado de la ciberseguridad en la región ..... 25

**4.5 MARCO LEGAL** ..... **26**

Ley 603 de 2000 ..... 26
Ley estatutaria 1266 (31 dic 2008) ..... 26
Ley 1273 del 5 de enero de 2009 ..... 26
Ley 1341 (30 jul 2009) ..... 27
Ley estatutaria 1581 de 2012 ..... 27

*5 DISEÑO METODOLÓGICO* ..... *27*

**5.1 Tipo de investigación a utilizar** ..... **27**

**5.2 TECNICAS PARA LA RECOLECCION DE LA INFORMACION** ..... **28**

**5.3 Instrumentos a utilizar en la recolección de los datos** ..... **28**

**5.4 Analizar la información recolectada** ..... **29**

*6 DESARROLLO DE LOS OBJETIVOS ..... 30*

**6.1 Establecer la metodología adecuada para un hacking ético, mediante el análisis documental con el fin de conocer sus características, ventajas, desventajas y contextos de aplicación ..... 30**

(INFORMATION SYSTEMS SECURITY ASSESSMENT FRAMEWORK) ISSAF ..... 30
OS (OFFENSIVE SECURITY) ..... 31
OWASP (OPEN WEB APPLICATION SECURITY PROJECT) ..... 33
METODOLOGIA SELECCIONADA OS (OFFENSIVE SECURITY) ..... 35

**6.2 Desarrollar la metodología de hacking ético seleccionada al Sistema de seguridad de la información de la entidad PIJAOS SALUD EPS INDIGENA sede Ibagué, con el fin de identificar las vulnerabilidades y amenazas a las cuales se encuentra expuesto ..... 36**

Fases de Trabajo e Implementación OS (OFFENSIVE SECURITY) ..... 36
POLITICAS DE SEGURIDAD DE LA EPS INDIGENA PIJAOS SALUD. ..... 42
Siguiente fase de aplicación de OS (OFFENSIVE SECURITY) intrusiones y hacking ético. ..... 43

**6.3Diseñar un informe que relaciones los controles que permitan mitigar el riesgo asociado a las vulnerabilidades identificadas para una correcta gestión de confidencialidad, integridad y disponibilidad de la información de la organización ..... 55**

*7 CONCLUSIONES ..... 56*

*8 RECOMENDACIONES ..... 58*

*9 BIBLIOGRAFÍA ..... 60*

*ANEXOS ..... 63*

## LISTA DE ILUSTRACIONES

Pág.
Ilustración 1 Pasos de ejecución de OS....32
Ilustración 2 Ejemplo Metodología OWASP....35
Ilustración 3 Cuestionario Ciberseguridad....38
Ilustración 4 Pregunta 1....38
Ilustración 5 Pregunta 2....39
Ilustración 6 Pregunta 3....39
Ilustración 7 Pregunta 4....40
Ilustración 8 Pregunta 5....40
Ilustración 9 Pregunta 6....41
Ilustración 10 Pregunta 7....41
Ilustración 11 Pregunta 8....42
Ilustración 12 Caratula Manual de Políticas de Seguridad de la Información....42
Ilustración 13 Nmap....44
Ilustración 14 Kali Linux....44
Ilustración 15 Meta Exploits....45
Ilustración 16 Escaneo -sS TCP SYN....46
Ilustración 17 Comando –sS....47
Ilustración 18 Resultado del Escaneo -sS....47
Ilustración 19 Comando -sS -sV....48
Ilustración 20 Resultado Comando -sS -sV....48
Ilustración 21 Servidor Windows Server 2012 R2....49
Ilustración 22 IP Servidor....50
Ilustración 23 Ping al Servidor....50
Ilustración 24 Inicio de trabajo con Metasploit....51
Ilustración 25 set a IP del Server....51
Ilustración 26 Corremos el Escaneo a la IP del Server....52
Ilustración 27 Vulnerabilidad Encontrada....52
Ilustración 28 Uso de la Vulnerabilidad....53
Ilustración 29 Cambio de Puerto....53
Ilustración 30 Ataque Finalizado....54

## LISTA DE CUADROS

pág.

Cuadro 1 Herramientas ISSAF .....31
Cuadro 2 Pasos Metodología OS .....33
Cuadro 3 Comparativa Metodologías .....35
Cuadro 4 Versionado del Manual.....43

## LISTA DE ANEXOS

pág.

Anexo 1. Informe Controles .....63

## GLOSARIO

**Continuidad del negocio**: Este concepto se refiere directamente a un Plan orientado a permitir la continuación de las principales funciones de la entidad sin generar más riesgos.

**Incidente de Seguridad:** Este es un evento adverso, que se puede confirmar o del cual se tiene sospecha, que se encargue de vulnerar la seguridad de la información, esto sin importar de la información que sea afectada, o la plataforma tecnológica, tampoco de la frecuencia, ni de las consecuencias, comprometiendo las diferentes operaciones de la EPSI y amenazar la seguridad de la información.

**Ingeniería Social**: Esta es una técnica utilizada con la manipulación de usuarios con la finalidad de conseguir que ellos hagan debilitar la seguridad de una red o lograr que faciliten información clasificada inconscientemente.

**Propietario de la información**: Habla directamente del proceso donde se crean los activos de información.

**Política de seguridad:** Documento que establece el compromiso de la Gerencia y el enfoque de la EPSI en la gestión de la seguridad de la información.

**Recursos tecnológicos**: Se refiere a todos aquellos componentes de software y hardware, que se tengan dentro de una organización entre ellos, servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros

**Registros de Auditoría**: Estos son los archivos donde se realizan los registrados de los eventos que se han identificado en los sistemas de información de la entidad, Entre estos eventos se pueden identificar intentos de accesos fallidos y exitosos, diferentes cambios a la configuración, uso de utilidades y también fallas de los sistemas entre muchos otros.

**Responsable por el activo de información**: Este es el funcionario que se encuentra a cargo de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y pidiendo tomar la decisión de cómo usar, identificar, clasificar y proteger dichos activos a su cargo.

**Riesgo**: Este entre otros es una gran posibilidad de que una amenaza logre ser explotada en una vulnerabilidad causando una gran pérdida o daño en los activos de información combinando la probabilidad de un evento y sus consecuencias.

**Seguridad de la información**: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

**SGSI**: “Sistema de Gestión de Seguridad de la Información”.

**Software malicioso**: Este concepto abarca gran variedad de software o programas de códigos intrusivos que siempre buscan como objeto ingresar y dañar los sistemas operativos, recursos tecnológicos, sistemas de información y redes de datos.

**Tratamiento de riesgos**: Esta es un documento de gestión que muestra las alternativas que utilizaremos para la prevención, de los riesgos en la seguridad de la información indicándonos los controles necesarios.

## RESUMEN

El análisis que se va a realizar al sistema de seguridad de la información dentro de la EPSI PIJAOS SALUD sede Ibagué, Tolima estará enfocado principalmente al hallazgo de las diferentes vulnerabilidades de seguridad que se puedan llegar a encontrar, teniendo como partida el enfoque de seguridad de la información dado desde el área encargada de este dentro de la entidad PIJAOS SALUD EPSI sede Ibagué, Tolima. Los activos tecnológicos son los encargados de almacenar la información de la entidad, esa información que es tan vital para la continuidad del negocio. Por tal motivo se debe tener en cuenta que la seguridad informática dentro de las organizaciones necesita tener estrategias y metodologías que logren garantizar los tres pilares fundamentales de la seguridad informática, que son integridad, confidencialidad y disponibilidad de la información.

Con la realización de este análisis al sistema de seguridad de la información de la entidad y priorizando el hallazgo de las vulnerabilidades en el sistema de información por medio de hacking ético para aclarar con este hallazgo que acciones tomar, ayudando a establecer correctivos e imponer controles más adecuados, cerrando las puertas a posibles situaciones que pongan en riesgo el activo más preciado que es, su información.



**Palabras claves:** Confidencialidad, disponibilidad, integridad, vulnerabilidad.

## ABSTRACT

The analysis that will be carried out on the information security system within the EPSI PIJAOS SALUD headquarters Ibagué, Tolima will be focused mainly on the discovery of the different security vulnerabilities that may be found, taking as a starting point the security approach of the information given from the area in charge of this within the entity PIJAOS SALUD EPSI headquarters Ibagué, Tolima. The technological assets are in charge of storing the entity's information, that information that is so vital for the continuity of the business. For this reason, it must be taken into account that computer security within organizations needs to have strategies and methodologies that are able to guarantee the three fundamental pillars of computer security, which are integrity, confidentiality and availability of information.

By carrying out this analysis of the entity's information security system and prioritizing the discovery of vulnerabilities in the information system through ethical hacking to clarify with this finding what actions to take, helping to establish corrective measures and impose more controls. Adequate, closing the doors to possible situations that put at risk the most precious asset that is, your information.



**Keywords:** Availability, confidentiality, integrity, vulnerability.

# INTRODUCCIÓN

El presente documento nos da un recorrido por el trabajo de grado aplicado, que fue propuesto, para el estudio realizado a la seguridad del sistema de información de la entidad pública de carácter especial Pijaos salud EPS Indígena. Para ejecutar correctamente este estudio se encaminaron una serie de procedimientos con el fin de ejecutar el trabajo de grado aplicado y así obtener resultados más óptimos, entre los procedimientos realizados se encuentra el planteamiento del problema que es la fuente principal del estudio ya que gracias a este planteamiento se da un norte al trabajo de grado aplicado, exponiendo la verdadera razón por la cual se elabora este documento.

Una vez se expone el problema se inicia con la selección de metodologías a utilizar con la finalidad real de buscar estrategias y diferentes alternativas que logren dar una solución a dicha problemática. Dándonos a conocer los distintos argumentos y razones que se utilizaran para adelantar el estudio, con el fin de poder cumplir los objetivos propuestos a cabalidad. Si bien es muy importante el lograr proponernos unos objetivos y plantearnos una problemática, también lo es relacionar los diferentes datos, teorías e investigación recopilados con el fin de dar una base fuerte para nuestro estudio, incluyendo las diferentes metodologías utilizadas, estrategias de seguridad y cualquier otro factor que puedan resultar útiles.

No obstante, es de suma importancia tener en cuenta el hecho de plantear una metodología de estudio que cumpla con el desarrollo efectivo a la solución de las problemáticas encontradas y planteadas en este documento, consistentemente en el estudio es necesario utilizar de manera correcta las diferentes metodologías, herramientas e instrumentos que se vayan a trabajar. También durante el desarrollo del documento podemos encontrar y observar los resultados obtenidos por el estudio inicial, estructurando con estos resultados un diagnostico que conlleve a la resolución de la problemática que se encuentre.

En el documento también estará plasmada toda aquella información relevante para la solución de problemáticas similares y estará documentada de la manera adecuada toda aquella información que conlleve a un diagnóstico adecuado y una respuesta congruente con la problemática que se haya planteado. Finalizando el documento con sus respectivas conclusiones y con las diferentes recomendaciones que se logran obtener durante el desarrollo del estudio.

# 1. DEFINICIÓN DEL PROBLEMA

## 1.1 ANTECEDENTES DEL PROBLEMA

Pijaos Salud es una Entidad Promotora de Salud Indígena de carácter especial, que presta sus servicios al sector indígena del departamento del Tolima perteneciendo íntegramente al sector público especial de la salud en Colombia. Por esta razón y teniendo en cuenta que en la mayoría de los casos la seguridad de la información es el talón de Aquiles de las diferentes entidades públicas del sector salud en Colombia, debido a la pobre gestión que se realiza en cuanto a sus infraestructuras informáticas internas, sus redes, sus bases de datos y de más activos de información con los que cuentan. Esto hace que cada vez se vuelvan más y más vulnerables frente al gran crecimiento tecnológico que están teniendo los ciberdelincuentes en el país, poniendo en riesgo latente cada día su información y la continuidad del negocio que es la gestión de los recursos destinados por el gobierno para la salud para la población indígena del departamento del Tolima.

Una vez expuesto el contexto y teniendo en cuenta también que la mayoría de las empresas infectadas con ransomware ya contaban con una solución de seguridad informática. Se logra identificar que una de las faltas más graves en cuanto a la seguridad de información se refiere, es el poco conocimiento técnico en el ámbito de seguridad de la información por parte de los encargados de salvaguardar los activos de información en la entidad. Otro de los problemas que podemos encontrar es la falta de liderazgo y apropiación de las diferentes técnicas que se podrían usar para la detección y prevención de intrusiones no autorizadas que deberían estar dentro del sistema de seguridad de la información que se está implementando dentro de la EPS INDIGENA.

Teniendo en cuenta que actualmente, PIJAOS SALUD EPSI se encuentra expuesta a las distintas amenazas en la red, abarcando posibilidades de que ocurran eventos que causen daños considerables dentro del sistema de información, otra de las causas de esta problemática se presenta también, por lo relevante de la información que se maneja sobre cada usuario que pertenece a la EPS INDIGENA, información personal, datos de contacto, tipo de etnia, resguardos a los que pertenecen y recursos que son administrados por la EPS INDIGENA. Toda esta es información que en gran medida puede llamar la atención de la ciberdelincuencia es un altísimo indicador de riesgo, sin contar la falta de recursos tecnológicos apropiados para mantener segura esta información, la falta de recurso humano preparado y capacitado en seguridad de la información que le permita a esta EPS INDIGENA contar con un sistema de seguridad más eficiente y confiable con buenas condiciones que logren reducir la exposición a las amenazas y ataques futuros.

## 1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo diagnosticar correctamente, la seguridad de la información en la EPS INDIGENA PIJAOS SALUD mediante el uso de metodologías de hacking ético?

# 2 JUSTIFICACIÓN

La gran expansión tecnológica que ha tenido el país en los últimos años ha traído consigo también grandes problemas en materia de seguridad informática, debido a que a la medida en que las grandes organizaciones se han puesto en la tarea de mejorar sus sistemas de información para salvaguardar sus activos de información y blindarse contra las distintas amenazas que puedan surgir en este nuevo tablero de juego, todo esto apoyados en las diferentes normas y adoptando políticas de seguridad de la información que puedan cumplir con el propósito de mantenerlos seguros frente a la ola de riesgos y amenazas latentes en la red. Los ciberdelincuentes también se han puesto en la tarea de hacerlo. “Dada la situación que vive el mundo, los ciberdelincuentes sacan provecho para hacerse pasar por organismos, infectar sistemas o conseguir datos.”[1]

PIJAOS SALUD EPS INDIGENA siendo una organización de salud pública de carácter especial se encuentra en la obligación de salvaguardar de la mejor manera los activos de información que resultan ser fundamentales para la continuidad del negocio, entre ellos las bases de datos en las cuales se aloja la información sensible de sus usuarios y demás información que pueda llegar a ser objeto de algún daño amenaza o ataque por parte de terceros ajenos a la entidad o propios también que busquen realizar algún tipo de intrusión no autorizada en el transcurso del ejerció de transportar y almacenar dicha información en la red. En aras de evitar todas estas situaciones es de suma importancia cumplir con ciertas “políticas de seguridad y seguir mejores prácticas. Para esto, el equipo gerencial debe ser el primero en establecer la protección de datos como una prioridad para la institución, dar ejemplo, capacitar a sus empleados y exigir que se cumplan los protocolos.”[2]

Los diagnósticos a tiempo son una de las herramientas más útiles para poder defender nuestros sistemas de información de ataques que puedan ocurrir. Realizando los análisis se podría determinar el nivel real de la seguridad y de la privacidad que se tiene de la información, permitiendo con una detección temprana el poder considerar el desarrollo de un plan de seguridad adecuado que logre reducir el riesgo, al implementar controles y seguimientos para conseguir los ajustes necesarios que eviten perdida o intrusión en la privacidad de nuestra información. No obstante a los análisis y diagnósticos también se debe tener en cuenta que “Se debe tener a toda la compañía bajo un antivirus pago que despliegue los antivirus

[1] LR, LA REPUBLICA, Colombia ocupa el puesto 39 en el ranking mundial sobre ciberseguridad. [EN LÍNEA]. 02 junio 2020. [Citado en 08 de octubre de 2021]. Disponible en internet: < https://www.larepublica.co/globoeconomia/ciberseguridad-otro-reto-que-deben-enfrentar-las-empresas-en-el-mundo-por-covid-3013083>

[2] MONROY, Sergio. Protección de datos en hospitales: Políticas de seguridad informática. [EN LÍNEA]. 26 junio 2019. [Citado en 08 de octubre de 2021]. Disponible en internet: < https://dondoctor.com/sector-salud-colombia/proteccion-de-datos-en-hospitales-10-politicas-de-seguridad-informatica/>

en todos los equipos y dispositivos móviles para que toda la información tenga la seguridad."[3]

Por este tipo de razones se hace indispensable y totalmente necesario el poder ejecutar un análisis adecuado con la metodología de hacking ético en el sistema de seguridad de la información de la EPS INDIGENA PIJAOS SALUD. Asegurando con este análisis y sus resultados buscar una forma adecuada de mantener la seguridad de la información en la entidad analizada.

[3] LR, LA REPUBLICA, Colombia ocupa el puesto 39 en el ranking mundial sobre ciberseguridad. [EN LÍNEA]. 02 junio 2020. [Citado en 08 de octubre de 2021]. Disponible en internet: < https://www.larepublica.co/globoeconomia/ciberseguridad-otro-reto-que-deben-enfrentar-las-empresas-en-el-mundo-por-covid-3013083>

# 3 OBJETIVOS

## 3.1 OBJETIVOS GENERAL

Evaluar el sistema de seguridad de la información de la entidad PIJAOS SALUD EPS INDIGENA sede Ibagué, mediante la implementación de técnicas de Hacking ético para determinar los controles más apropiados que permitan gestionar la confidencialidad, integridad y disponibilidad de la información de la organización.

## 3.2 OBJETIVOS ESPECÍFICOS

• Establecer la metodología adecuada para un hacking ético, mediante el análisis documental con el fin de conocer sus características, ventajas, desventajas y contextos de aplicación.

• Desarrollar la metodología de hacking ético seleccionada al Sistema de seguridad de la información de la entidad PIJAOS SALUD EPS INDIGENA sede Ibagué, con el fin de identificar las vulnerabilidades y amenazas a las cuales se encuentra expuesto.

• Diseñar un informe que relaciones los controles que permitan mitigar el riesgo asociado a las vulnerabilidades identificadas para una correcta gestión de confidencialidad, integridad y disponibilidad de la información de la organización.

# 4 MARCO REFERENCIAL

## 4.1 MARCO TEÓRICO

**4.1.1 Referente Bibliográfico** En el Repositorio de la facultad de Ciencias de la Computación y Electrónica de la UTA (Universidad Tecnológica Americana) se puede encontrar un trabajo de tesis con similares características titulado "HACKING ÉTICO PARA DETECTAR VULNERABILIDADES EN LOS SERVICIOS DE LA INTRANET DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN CEVALLOS."[4], el cual fue desarrollado por: Gloria Nataly Huilca Chicaiza en el año 2012, como Seminario de Graduación previo a la obtención del título de ingeniera en Sistemas Computacionales e Informáticos.

**4.1.2 Importancia del hacking ético en una organización** "El hacking ético ha adquirido una importancia creciente en los últimos años ante el rápido aumento de los casos de ciberdelincuencia. Cada vez más empresas, organizaciones e instituciones buscan expertos en ciberseguridad que puedan testar su propio concepto de seguridad actuando como atacantes reales."[5]

Las amenazas constantes de ciberataques se han convertido en el diario vivir de muchas de las organizaciones que no cuentan con un sistema adecuado ni cumplen los parámetros en cuanto a una directiva encaminada a la seguridad de su información. Todos sabemos que frente a las amenazas informáticas, el espectro de conocimiento se ha tornado muy amplio ya que los atacantes empezaron a lucrarse de sus delitos informáticos y se convirtieron en una empresa criminal que sigue buscando cada día la manera más fácil de escabullirse en nuestros sistemas y hacer daño a nuestra información. Aunque el panorama no es muy alentador para algunas organizaciones que no han hecho el esfuerzo necesario para blindar sus sistemas de información contra este flagelo, otras organizaciones si se comprometieron en hacer bien la tarea y estar a la vanguardia de herramientas de hardware y software que puedan hacer frente a cualquier ataque o intrusión maliciosa en sus sistemas.

**4.1.3 Amenazas informáticas.** La tecnología en la actualidad ha revolucionado un cambio sorprendente, se ha desarrollado de una manera tan fuerte que le ha dado la posibilidad a los sectores tanto públicos como privados tener acceso al instante a cualquier tipo de información, siendo esta una situación bastante favorable, ya

[4] HUILCA, Gloria Nataly, Tesis_t764si.pdf - Repositorio Universidad Técnica de Ambato. [EN LÍNEA].22 noviembre 2012. [Citado en 22 de abril de 2021]. Disponible en internet: <https://repositorio.uta.edu.ec/bitstream/123456789/2900/1/Tesis_t764si.pdf

[5] DIGITAL GUIDE, Ethical hacking: solucionar fallos de seguridad y prevenir la cibercriminalidad. [EN LÍNEA].06 noviembre 2020. [Citado en 09 de octubre de 2021]. Disponible en internet: <https://www.ionos.es/digitalguide/servidores/seguridad/que-es-el-ethical-hacking/>

que gracias a esta actualización tecnológica se podrían resolver problemas de manera mucho más rápida y eficiente, no siendo todo bueno ya que de igual manera se debe tener presente de la gran cantidad de amenazas que acarrea el tener que enfrentarse a diario con el avance tecnológico que también ha tenido la ciber delincuencia, el mantener segura nuestra información y tener la posibilidad de bloquear ataques entre otras amenazas es lo que tenemos que afrontar ahora que la tecnología avanza tan rápidamente.

El análisis de vulnerabilidades utilizando técnicas de penetración y hacking ético conllevan en lograr un análisis más profundo al sistema e información de la organización atacando de una forma pasiva el entorno de seguridad que ha creado dentro de la entidad, el objetivo que se tiene es ponerse en los zapatos de los atacantes reales para poder detectar que vulnerabilidades se puedan encontrar ya que si fuera un escenario real el atacante también encontraría dichas vulnerabilidades y las explotaría de forma que no podríamos detener una intrusión y lograrían el cometido de atacar y poner en riesgo la información y el sistema como tal. Con este tipo de análisis utilizando la técnica de hacking ético se logra identificar la configuración que se tiene en cuanto a la seguridad del sistema y que se puede llegar a configurar si el caso es que resulta negativo el diagnóstico de la prueba.

**4.1.4 Beneficios del Hacking ético** El hacking ético está principalmente enfocado en poder prevenir cualquier ataque que pueda afectar nuestros sistemas de información, imitando escenarios que en algún momento podrían ocurrir, con estas pruebas nos preparan para qué si en algún momento sucede realmente este ataque se pueda reaccionar de la manera adecuada, dando con este tipo de simulaciones la facilidad de adelantarnos a ataques reales con el resultado de los análisis permitiendo a las organizaciones estar preparados.

Debemos tener en cuenta también que el hacking ético brinda la realización de pruebas, las cuales pueden albergar las pruebas de caja negra, las de caja gris y las pruebas de caja blanca también. Teniendo en contexto que estas pruebas de pentesting se catalogan como la manera más fácil y eficaz para identificar la seguridad de información del sistema, porque con estas se utilizan herramientas muy similares a las que utilizan los atacantes en la realidad, diferenciando que estos ataques so de pruebas y realizados siempre bajo ambientes controlados sin afectar ningún componente del sistema.

**4.1.5 Pruebas de penetración de Caja blanca** Es uno de los informes más sencillos de realizar y necesita información de las personas que tienen un conocimiento completo sobre los datos de la red.

**4.1.6 Pruebas de penetración de Caja negra** En esta técnica se realiza desde cero el ingreso ya que no se suministra ningún tipo de información a la persona que está realizando la prueba, consiguiendo con esto un informe más completo sobre

las vulnerabilidades que se presentan realmente en el sistema garantizando un resultado más exacto.

**4.1.7 Pruebas de penetración de Caja gris** En este método se combinan los dos anteriores caja blanca y caja negra y brinda una información parcial del estado del sistema, se usa principalmente para auditar una parte del proceso en particular.

Con la información adquirida sobre las diferentes técnicas y metodologías a utilizar se puede desarrollar un análisis del sistema con fundamentos más estables esperando resultados más acertados sobre el verdadero estado de la seguridad de la información de la EPS INDIGENA PIJAOS SALUD. Con estos fundamentos más claros y establecidos se podría generar un informe más robusto sobre las diferentes vulnerabilidades y amenaza que pudieran afectar el activo de información de la entidad.

## 4.2 MARCO CONCEPTUAL

Con el fin de dar un norte a este proyecto se deben realizar los análisis y mediciones directamente relacionadas con el concepto de vulnerabilidad, como también de amenazas en la seguridad informática, en el diagnóstico que se brinde una vez analizados los resultados se establecerá la confidencialidad, disponibilidad e integridad de la información de la EPS INDIGENA PIJAOS SALUD. Describiendo a continuación algunos de estos conceptos:

Hacking Ético: Es una referencia al estado de aprobación y aplicación de metodologías de hacking en una organización para analizar el sistema informático de manera legal y en un ambiente controlado.

Amenaza: Respecto al concepto que envuelve esta palabra podríamos indicar que “Una amenaza está directamente ligada a un incidente nuevo, recién descubierto con el potencial de causar un daño considerable en un sistema o empresa en general.”

Riesgo: “Particularmente los riesgos informáticos son aquellas exposiciones a las que se ven expuestos los sistemas tales como amenazas, atentados entre otros, a los sistemas de información.”

Vulnerabilidad: Teniendo el contexto que esto es una debilidad que se encuentra en un sistema de información y que esta será explotada por cualquier ciberdelincuente que la halle todo con el fin de acceder de clandestina y sin autorización en busca de cometer acciones prohibidas que puedan o no comprometer un sistema informático. “Las vulnerabilidades pueden permitir a los atacantes ejecutar código, acceder a la

memoria de un sistema, instalar malware y robar, destruir o modificar datos confidenciales."[6]

Confidencialidad: Este concepto indica que es la capacidad que se tiene en un sistema de poder garantizar que toda la información, almacenada en el mismo sistema o que es transportada por la red, estará disponible únicamente para los usuarios que se encuentran autorizados de recibirla, de allí la palabra confidencial.

Disponibilidad: "Este concepto se basa en la capacidad de poder garantizar que en conjunto el sistema y los datos alojados en el siempre van a estar disponibles al usuario en el momento de requerirlos."[7]

Integridad: "Decimos integridad a la capacidad de garantizar que se tiene para que los datos no estén modificados desde su creación sin que haya sido autorizado. Confirmando que la información que se tiene es válida y consistente con la original. "[8]

Controles: "Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal."[9]

Auditoria: es un proceso independiente realizado sistemáticamente que se documenta con el fin de obtener las evidencias necesarias de dicha auditoria para posteriormente analizarlo con la guía de auditoria de la ISO 2700.

Activo de información: "Un activo de información en el contexto de la norma ISO/IEC 27001 es algo que una organización valora y por lo tanto debe proteger."[10]

[6] ORTIZ, Ángel. ¿Qué es una vulnerabilidad en seguridad informática? [EN LÍNEA].2020. [Citado en 09 de octubre de 2021]. Disponible en internet: < https://www.hostdime.com.pe/blog/que-es-una-vulnerabilidad-en-seguridad-informatica-ejemplos/>

[7] SEGURIDAD INFORMATICA. Objetivos de la seguridad informática [EN LÍNEA].2020. [Citado en 09 de octubre de 2021]. Disponible en internet: < https://infosegur.wordpress.com/tag/confidencialidad/>

[8] SEGURIDAD INFORMATICA. Objetivos de la seguridad informática [EN LÍNEA].2020. [Citado en 09 de octubre de 2021]. Disponible en internet: < https://infosegur.wordpress.com/tag/confidencialidad/>

[9] MINTIC. Seguridad y Privacidad de la Información. [EN LÍNEA].2016. [Citado en 09 de octubre de 2021]. Disponible en internet: < https://mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf/>

[10] CARDENAS, Fabián. ¿Qué es la gestión de activos de información?. [EN LÍNEA].2020. [Citado en 09 de octubre de 2021]. Disponible en internet: < https://www.novasec.co/blog/67-gestion-de-activos-de-informacion/>

## 4.3 MARCO HISTÓRICO

Teniendo de marco esta perspectiva, es bastante pintoresco el pobre intento de los medios de comunicación, de dar una explicación a un concepto que si bien es cierto existe desde el inicio de la era digital resulta totalmente nuevo para ellos, los hackers son parte de este nuevo mundo tecnológico y junto con ellos todo lo que conlleva su actuar en el sistema. Hacking una palabra que tiene sus orígenes relacionados con la aparición del teléfono, este término que tuvo sus orígenes entre 1950 y 1960 relacionado con el instituto tecnológico de Massachusetts (MIT).

En la web se pueden encontrar algunas teorías donde se describen ciertas prácticas utilizadas como hacking entre ellas esta una teoría describiendo hace algunos años, "en el MIT era utilizada la palabra "hack" para definir una solución simple, creativa y elegante para un problema."[11]

También encontramos otra de las teorías que indica que "Un club de maquetas de trenes, luego de recibir una donación de componentes, que en su gran mayoría eran de equipos telefónicos, desarrollaron un sistema que permitía a múltiples operarios controlar diferentes tramos de las vías utilizando el teléfono para comunicarse con las secciones adecuadas. Denominando esta labor como hacking."[12]

Es encontrada en la web además de las 2 teorías anteriores otra donde se enfoca en la compañía AT&T, la cual, en 1878, contrato a unos muchachos para trabajar allí en el área de telefonía, "lo cual resultó ser un desastre ya que estos preferían curiosear que hacer su trabajo, y entre otras cosas comenzaron a hacer bromas a los clientes, desconectando llamadas o bien cruzando líneas, por lo que los clientes terminaban hablando con desconocidos. El cual daría forma a las primeras generaciones de hackers."[13]

## 4.4 ANTECEDENTES O ESTADO ACTUAL

**Estado de la ciberseguridad en la región.** Aunque parezca difícil de creer un 50 % de las organizaciones en Colombia se están preparando para enfrentar un ciberataque según un estudio realizado, "es cierto que Colombia sufre problemas significativos de ciberseguridad, aunque luego de realizar el estudio nos damos cuenta que esas falencias no son tan críticas comparadas con las falencias que tienen otros países de la región, e incluso del resto del mundo desarrollado. Este estudio fue entregado por Comparitech, una plataforma que se especializa en el

[11] Software Gurú, La Ética en el Hacking. [EN LÍNEA].2020. [Citado en 09 de octubre de 2021]. Disponible en internet: <https://sg.com.mx/revista/48/la-etica-el-hacking>
[12] Software Gurú, La Ética en el Hacking. [EN LÍNEA].2020. [Citado en 09 de octubre de 2021]. Disponible en internet: <https://sg.com.mx/revista/48/la-etica-el-hacking>
[13] Software Gurú, La Ética en el Hacking. [EN LÍNEA].2020. [Citado en 09 de octubre de 2021]. Disponible en internet: <https://sg.com.mx/revista/48/la-etica-el-hacking>

análisis de servicios tecnológicos. "[14] Tomando como base este estudio nos damos cuenta que Pijaos Salud EPS Indígena no puede ser la excepción y también se encuentra en este momento trabajando para la mejora de su seguridad Informática.

El facilitar el acceso a la información casi al instante y mantenernos informados en cualquier lugar y momento. Es una de las ventajas más grandes que se tiene en este momento gracias al avance de la tecnología, sin embargo, se debe tener en cuenta que todos estos datos no son verdadero conocimiento ni sabiduría de quienes acceden a dicha información. Es de conocimiento que la sociedad en la que actualmente vivimos es una sociedad de consumo que por su acercamiento a este nuevo mundo tecnológico cuenta con todas las facilidades para mantener en conexión constante y mantener informados carece de la madurez suficiente para utilizar este conocimiento de la manera adecuada.

"El uso del hacking ético en Pijaos salud EPS Indígena conllevan a múltiples beneficios, una vez se logra establecer la forma de uso correcto dentro del análisis a desarrollar, se puede evidenciar que con el uso de la metodología de Ética hacking Pijaos salud EPS Indígena podrá ahorrar dinero realizando la actualización de sistemas de seguridad más eficientes, también se podrían impedir catástrofes futuras por ser víctima de algún tipo de ataque hacker, manteniendo y organizando los sistemas de ciberseguridad para evitar infiltraciones.

## 4.5 MARCO LEGAL

**Ley 603 de 2000**. Esta es una ley que indica los parámetros acerca de la protección de los derechos de autor en Colombia. Entre ellos podemos incluir también la creación de software ya que es un activo, protegido y obligando a las entidades a realizar la declaración legal del software instalado cualquier equipo de la entidad.

**Ley estatutaria 1266 (31 dic 2008)**. Esta ley se encarga de indicar información general sobre el Hábeas Data, regulando el manejo de todos los datos que están contenidos en las bases de datos, primordialmente en las bases de datos financieras, bases crediticias, bases comerciales, y de servicios, también las que provienen de otros países.

**Ley 1273 del 5 de enero de 2009.** Con esta ley se encargaron de modificar "el Código Penal, información y de los datos"- preservando completamente las tecnologías de la información y de las comunicaciones.

[14] PROFITLINE, Actualmente Como se encuentra Colombia en Seguridad Informática. [EN LÍNEA].26 febrero 2019. [Citado en 09 de octubre de 2021]. Disponible en internet: <https://profitline.com.co/actualmente-como-se-encuentra-colombia-en-seguridad-informatica/>

**Ley 1341 (30 jul 2009).** Ley en la que se realizan las definiciones de los conceptos que hay con lineamientos hacia la sociedad informática y organizaciones de las distintas Tecnologías de las comunicaciones y la información que existen –TIC.

**Ley estatutaria 1581 de 2012**. Esta ley inicia su vigencia el 17 de octubre 2012 para la protección de datos los personales, prohibiendo la transferencia de datos personales a cualquier país que no tenga reglamentada la seguridad de dicha información,

# 5 DISEÑO METODOLÓGICO

Con el fin de realizar un análisis al estado real de la seguridad del sistema de información de la EPS INDIGENA PIJAOS SALUD poder identificar las vulnerabilidades y amenazas que se presentan, es necesario tener claro el personal que se ve involucrado en el proceso de resguardar la información por parte de la entidad, los encargados de manipular el sistema y que privilegios tienen respecto a los cambios que se puedan generar dentro del sistema de información. Para lograr este objetivo se realizan algunas consultas dentro de la entidad, se reúne al personal involucrado para determinar el estado real y la capacitación que tienen en cuanto a seguridad de la información.

Una vez se realiza un levantamiento inicial de dicha información se procede a dar inicio con el análisis detallado del sistema utilizando diferentes técnicas de hacking ético y penetraciones, que hacen parte del proceso de identificación de riesgos en las organizaciones, con el fin de lograr identificar y abordar de manera sistemática los riesgos que se vayan localizando. Pretendiendo con esto empezar a articular diferentes estrategias de cara a poder apropiar algunas metodologías que se encarguen de asegurar la seguridad de la información que contienen dentro del sistema, permitiendo con esto alcanzar un modelo acorde a las diferentes necesidades que tiene la entidad en materia de seguridad de la información. Permitiendo así identificar las infraestructuras críticas de la EPS INDIGENA y mejorar la respuesta ante cualquier amenaza que pueda afectar su seguridad.

## 5.1 TIPO DE INVESTIGACIÓN A UTILIZAR

En este proyecto se realiza un análisis profundo acerca del estado de la seguridad de la información en Pijaos Salud EPS Indígena y para ello se utiliza un tipo de estudio que permita la recopilación de los datos que se requieren de forma cuantitativa y descriptiva, esto con la finalidad de poder realizar el análisis deseado, mediante la utilización de las metodologías de hacking Ético. Permitiendo con este estudio poder identificar las diferentes características encontradas, señalando las

formas de conducta y actitud del universo a estudiar, logrando identificar la diferente información que será tomada por los distintos medios, observando, encuestas y las distintas listados de chequeo utilizados regularmente en este tipo de estudios.

## 5.2 TECNICAS PARA LA RECOLECCION DE LA INFORMACION

Para este proyecto se utiliza como fuente primaria la misma información que se logre recopilar directamente de la Sede Ibagué de Pijaos Salud EPS Indígena, trabajando los diferentes medios tales como son observación en sitio, también encuestas realizadas a los funcionarios de la entidad y las listas de chequeo abarcando las condiciones de cómo se encuentran las instalaciones tanto física como tecnológicamente.

En cuanto a las fuentes segundarias se trabaja tomando la documentación que se halle sobre SGSI, entre libros y documentos a fines, también se tomaran las bases de datos de la entidad Pijaos salud EPS Indígena, la normativa y los diferentes artículos que se logren encontrar sobre la gestión protección de datos.

## 5.3 INSTRUMENTOS A UTILIZAR EN LA RECOLECCIÓN DE LOS DATOS

Entre los instrumentos a utilizar se encuentran las fichas técnicas, Encuestas, listas de chequeo y observación directa en sitio.

Utilización de fichas técnicas: Con la finalidad de dar un orden y organizar de la manera adecuada la información de los distintos artículos, proyectos y libros que se van a utilizar sobre la correcta implementación del hacking Ético en un análisis de un sistema de información.

Utilización de encuestas: para estas encuestas se tendrá en cuenta la aplicación de encuestas estructuradas que contengan opciones de respuestas de selección múltiple con el fin de recolectar la información acerca de los verdaderos conocimientos, habilidades y experiencia de los distintos funcionarios de la entidad Pijaos Salud EPS Indígena sede Ibagué que serán encuestados.

Utilización de las Listas de chequeo: Para este paso se realiza una lista de chequeo para lograr identificar el estado en el que se encuentra actualmente la infraestructura tanto física como tecnológica de la entidad, esto con el fin de poder valorar los posibles riesgos que se vean inmersos y que atenten contra la seguridad de la información.

Utilización de la observación directa en sitio: Esta se realiza directamente con la finalidad de recopilar la mayor cantidad de información complementaria utilizando esta para lograr diagnosticar los sistemas de seguridad de la información de la

entidad Pijaos Salud EPS Indígena y para lograr identificar la metodología de hacking ético más conveniente.

## 5.4 ANALIZAR LA INFORMACIÓN RECOLECTADA

Toda la información que se recolecte en el avanzar del proyecto será procesada en hojas de cálculo basada en formulas y porcentajes con el fin de que sea mucho más comprensible y lograr su fácil interpretación. Para la interpretación de la información que se recolecte en las encuestas utilizaremos las diferentes graficas dinámicas enfocados en lograr discriminar de una mejor manera los resultados utilizando gráficos de tortas y tablas de porcentajes. Mientras en los resultados que se obtengan de las diferentes listas de chequeo lo resumiremos en gráficos de barras estableciendo los diferentes niveles de cumplimiento de los distintos requisitos técnicos para la seguridad de la información.

# 6 DESARROLLO DE LOS OBJETIVOS

## 6.1 ESTABLECER LA METODOLOGÍA ADECUADA PARA UN HACKING ÉTICO, MEDIANTE EL ANÁLISIS DOCUMENTAL CON EL FIN DE CONOCER SUS CARACTERÍSTICAS, VENTAJAS, DESVENTAJAS Y CONTEXTOS DE APLICACIÓN.

Con la finalidad de obtener los resultados para el respectivo análisis, se realizó la aplicación de una encuesta como fuente primaria de la información, permitiendo con esta la obtención de datos relevantes y resolver las dudas e inquietudes que se tiene sobre el tema de estudio, con la finalidad de implementar diferentes alternativas de solución a los problemas encontrados.

Todo esto se realiza para lograr determinar el estado actual de los sistemas de seguridad de la información de Pijaos Salud EPS Indígena sede Ibagué. Empleando las herramientas de seguridad de la información utilizando diferentes tipos de software que corren sobre el sistema operativo Linux, con el objetivo de hallar las vulnerabilidades en los sistemas de seguridad de la información implementados en la entidad. En la actualidad se cuenta con una gran cantidad de diferentes metodologías y herramientas que son utilizadas en el trabajo de evaluar las diferentes vulnerabilidades que se puedan encontrar en un sistema de información, en este análisis incluiremos las metodologías más importantes y que más son utilizadas ya que se reconocen a nivel mundial encontrando documentación suficiente de ellas.

### (INFORMATION SYSTEMS SECURITY ASSESSMENT FRAMEWORK) ISSAF

Realizando un reconocimiento de las metodologías de hacking ético encontramos la primera metodología ISSAF. Que se basa principalmente en una estructura de trabajo, capaz de dar modelado y evaluación a los requisitos que se encuentren dentro de los diferentes procesos que se llevan internamente en la seguridad de la información, definiendo de mejor manera un plan de pruebas, basándose en metodologías de dominios.

La ISSAF es una metodología que logra adoptar diferentes procesos en cuanto a tecnología de información se refiere, cubriendo distintos procesos de niveles más altos que se asocian directamente a las TICs. Lo usan principalmente las entidades financieras en sus procesos a nivel mundial. Sus procesos de evaluación lo hacen lo suficientemente fuerte ya que están con fundamentos firmes en desarrollar distintas etapas evaluativas en procesos auditores, incluyendo el pentesting, definiendo distintos espacios de evaluativos en cada uno de estos procesos.

La metodología ISSAF, se referencia toda en un marco de trabajo que define las políticas de evaluación de seguridad informática al igual que sus distintos procesos

dentro de las diferentes entidades, logrando integrar distintas herramientas, conformando un proceso de evaluación más robusto para las entidades. Definiendo herramientas de gestión y listas de control interno:

**Cuadro 1 Herramientas ISSAF**

| | control Metodologia ISSAF | |
|---|---|---|
| 1 | Evaluación de políticas y procedimientos de seguridad de la información en las empresas para reposte de cumplimiento de estándares industriales en TI y normatividad legal aplicable. | |
| 2 | Identificación y evaluación de áreas de comercio de servicios de infraestructuras que se prestan desde las áreas de TI. | |
| 3 | Desarrollar análisis de vulnerabilidades y pentesting para identificar vulnerabilidades que puedan representar algún riesgo potencial a cualquier activo de información de las organizaciones. | |
| 4 | Definir un modelo ideal de valoración por dominios de seguridad, con los cuales se pueda: | * Detectar alguna configuración problema y corregirla.<br>* Detectar riesgos asociados a las tecnologías instaladas y tratarlos.<br>* Determinar riesgos asociados a personal y a los procesos de negocio y tratarlos.<br>* Fortalecer procedimientos y tecnologías existentes en las organizaciones. |

Fuente: Propia

## OS (OFFENSIVE SECURITY)

En esta metodología podremos encontrar que ejecuta herramientas informáticas, principalmente aquellas enfocadas en ocasionar tropiezos en los diferentes sistemas informáticos, consiguiendo con este procedimiento conocer los diferentes huecos de seguridad que se puedan tener en nuestros sistema de información, con esta metodología se trabajara de una manera más fácil y centrada ya que se enfoca en utilizar las mismas herramientas que utilizan los atacantes en el momento de realizar sus ataques, todo esto lo realiza con el cuidado de no afectar directamente el sistema de información objeto de evaluación y de no alterar de ninguna manera la operación de la compañía mientras realiza su ataque.

Con esta metodología se puede medir el nivel real de seguridad que se tiene en el sistema de información de la entidad, ya que este permite confirmar mediante hallazgo directo si se encuentra alguna vulnerabilidad real, realizando diferentes ataques en ambientes controlados y generando una respuesta real de nuestro estado de seguridad, la ejecución de esta metodología se basa principalmente en una serie de pasos para lograr un resultado óptimo como se muestra a continuación en el siguiente gráfico:

## Pasos de ejecución de OS (OFFENSIVE SECURITY)

**Ilustración 1 Pasos de ejecución de OS**


Fuente: propia

Los pasos para la ejecución de la metodología OS se deben tener en cuenta para su correcto manejo, se relacionan a continuación el siguiente cuadro:

**Cuadro 2 Pasos Metodología OS**

| | Pasos de ejecución de Metodologia OS (OFFENSIVE SECURITY) |
|---|---|
| **Posicionamiento** | Se refiere a como se ubican el analista de seguridad o un determinado atacante con relación al objetivo de su análisis, las posiciones pueden ser internas o externas, lo cual define varios aspectos sobre lo que el cliente espera obtener. |
| **Visibilidad** | Hace referencia al tipo de información que se permite ver al analista, previamente a la ejecución del análisis, la información visible, incluye sistemas de información, archivos y documentación de la disposición de la red, esto define también, la posibilidad de conocer el nivel de exposición interno o externo hacia la información corporativa. |
| **Perfil Adoptado** | Aquí, se pueden definir varios perfiles según el tipo de análisis y la formación del atacante, y a su vez, también los define la necesidad del cliente, entre estos se podrían identificar usuarios que cuenten con suficientes privilegios en la red, que puedan acceder físicamente, o que no lo pueda hacer, también, puede ser un perfil avanzado o de conocimiento básico según sea la necesidad del usuario. |
| **Reconocimiento pasivo** | Normalmente el cliente hace entrega la información necesaria para la actividad, pero de igual forma se intenta conseguir información relacionada por otros medios, esta tarea, permite que se informe al cliente sobre la visibilidad de los objetivos propuestos desde afuera de la organización. |
| **Reconocimiento activo superficial** | Se identifican puntos-claves con relación directa al objetivo, con la idea de encontrar alguna actividad y posteriormente realizar análisis más profundos de los objetos encontrados. |
| **Reconocimiento activo en profundidad** | En este instante se usan los objetos identificados anteriormente para realizar una revisión o análisis profundo, aquí, se validan puertos, protocolos y servicios disponibles y principalmente, que tan actuales están sus aplicaciones y software instalado en estos. |
| **Análisis de vulnerabilidades** | Se inicia a determinar potenciales vulnerabilidades en la infraestructura instalada y sus componentes de software, es una etapa crítica de análisis, ya que se pueden presentar algunos falsos positivos a tratar. |
| **Explotación o ataque puro** | En esta etapa se desarrolla la explotación de vulnerabilidades encontradas en etapas anteriores, esto permite ejecutar código para su explotación y realizar mediciones finales. |
| **Consolidación** | Hasta este momento, ya existe un avance significativo del análisis y se da inicio a los procesos de intrusión, dejando comprometida alguna información, equipos o servicios que se lograron vulnerar. |
| **Borrado del rastro** | En esta etapa se debe eliminar cualquier tipo de rasgo que permita identificar una intrusión. |
| **Reportes** | Finalizando, esta etapa se da estructura a la información recolectada, generando informes de tipo Ejecutivo para la gerencia y de tipo técnico para las áreas de TIC y auditoria dentro de las organizaciones. |

Fuente: propia

## OWASP (OPEN WEB APPLICATION SECURITY PROJECT)

Esta metodología es un proyecto de código abierto basado en seguridad para aplicaciones web. Permitiendo a las entidades poder desarrollar distintos procesos dentro de la entidad entre ellos de seguridad informática, principalmente cuando se están desarrollando proyectos de desarrollo de software, ya que con estos proyectos las entidades se enfocan en aplicaciones web y servicios para la web. OWASP tiene diferentes herramientas que se disponen de forma gratuita para que sean utilizadas en cualquier momento, permitiendo a los usuarios hacer uso de sus foros, documentación y demás información que se publica de forma gratuita en la web. OWASP, principalmente busca resolver los problemas de seguridad en las diferentes aplicaciones, ya que esto se ha convertido en un problema recurrente en la creación y desarrollo de las mismas.

En este punto se analiza los beneficios del uso de La metodología OWASP (Open Web Application Security Project) Esta metodología está conformada por una comunidad totalmente abierta, que se colabora entre profesionales y entre expertos en la seguridad de las distintas aplicaciones Web. Este es uno de sus puntos más fuertes ya que gracias a ello se mantiene siempre en constante actualización. Se comparten entre muchas otras cosas diferentes guías de pruebas, diferentes manuales de referencias con diferentes vulnerabilidades, también "podemos encontrar en estos foros contramedidas y una muy completa metodología que nos sirve de ayuda para la revisión y posterior evaluación del estado de seguridad de nuestras aplicaciones desarrolladas o que tenemos en desarrollo."[15]

Los diferentes documentos y foros que se encuentran en la web sobre la metodología OWASP comparten además de información relevante también mucha otra de utilidad como:
Fragmento del contenido temático:

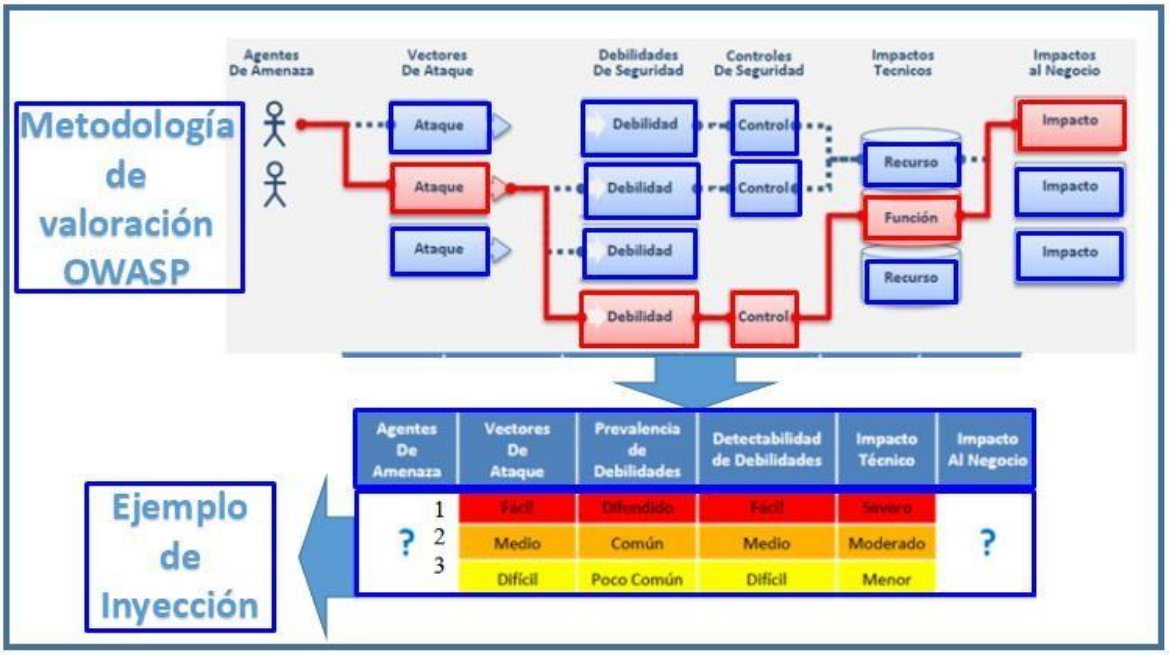
Se pueden encontrar las diferentes pruebas de intrusión de las aplicaciones Web, Robots, Spiders y Crawlers, También es fácil hallar pruebas de firmas digitales de diferentes aplicaciones web, el análisis de distintos códigos de error, al igual que pruebas de SSL/TLS, Archivos más antiguos, también copias de seguridad y que no tengan referencias, también encontramos los distintos métodos http y XST, Comprobaciones del sistema de autenticación, también encontramos transmisión de las credenciales por medio de un canal cifrado, también encontramos la enumeración de los usuarios, las cuentas de usuario que se pueden adivinar (por diccionario) O por Fuerza bruta, o por defecto, "pruebas de inyección de SQL, inyección de XML, las pruebas de desbordamiento de búfer, las Pruebas de HTTP

[15] DragonJAR. OWASP Testing Guide 3.0 en Español. [EN LÍNEA]. 26 junio 2019. [Citado en 20 de noviembre de 2021]. Disponible en internet: < https://www.dragonjar.org/owasp-testing-guide-3-0-en-espanol.xhtml/>

Splitting/Smuggling, y también Pruebas de denegación de servicio entre muchas otras. ”[16]

Se ha determinado que en las aplicaciones web la debilidad más común es la falta de una correcta validación de las diferentes entradas que proceden por parte del cliente o del entorno de la aplicación, llevando a vulnerar la seguridad de la aplicación, con inyecciones, ataques/Unicode, también desbordamiento de buffer entre otras, en la siguiente imagen se logra evidenciar el cómo se comporta una valoración de vulnerabilidad de la metodología OWASP:

**Ilustración 2 Ejemplo Metodología OWASP**




Fuente: propia

## METODOLOGIA SELECCIONADA OS (OFFENSIVE SECURITY)

**Cuadro 3 Comparativa Metodologías**

| (INFORMATION SYSTEMS SECURITY ASSESSMENT FRAMEWORK) ISSAF | OS (OFFENSIVE SECURITY) | OWASP (OPEN WEB APPLICATION SECURITY PROJECT) |
|---|---|---|
| Actúa principalmente como documentación de referencia de extremo a extremo para la Evaluación de seguridad. | Ejecuta herramientas informáticas, principalmente aquellas enfocadas en ocasionar tropiezos en los diferentes sistemas informáticos | Ofrece diferentes pruebas de intrusión de las aplicaciones Web |

[16] DragonJAR. OWASP Testing Guide 3.0 en Español. [EN LÍNEA]. 26 junio 2019. [Citado en 20 de noviembre de 2021]. Disponible en internet: < https://www.dragonjar.org/owasp-testing-guide-3-0-en-espanol.xhtml/>

| | | |
|---|---|---|
| Brinda una línea base para realizar una evaluación de seguridad | Permite conocer los diferentes huecos de seguridad que se puedan tener en nuestros sistema de información | Permite hallar pruebas de firmas digitales de diferentes aplicaciones web |
| Es principalmente un referente para la implementación de la seguridad de la información. | se puede medir el nivel real de seguridad que se tiene en el sistema de información | Se enfoca en desarrollar distintos procesos dentro de la entidad entre ellos de seguridad informática, principalmente cuando se están desarrollando proyectos de desarrollo de software |
| Brinda en esencia el fortalecimiento para procesos y tecnologías existentes. | Se pueden realizar diferentes ataques en ambientes controlados generando una respuesta real de nuestro estado de seguridad. | Se direcciona principalmente en resolver los problemas de seguridad en las diferentes aplicaciones. |

Una vez se realiza el estudio de comparativo de las diferentes metodologías respecto a las etapas del Ethical Hacking, se realiza la elección de la metodología **OS (OFFENSIVE SECURITY)** según las necesidades de la entidad, sus características, ventajas, desventajas y contextos de aplicación, tomando la decisión de determinar los diferentes tipos de pruebas que se deben realizar y los diferentes tipos de servicios que se deben revisar, especificando las obligaciones del proceso de pentesting a implementar. Definiendo los alcances de las pruebas, las limitaciones de las mismas en termino de acciones a realizar y resultados que se desean esperar, definiendo los criterios y procedimientos, e identificando los requisitos para el cumplimiento adecuado del estudio, características que se logran encontrar en la metodología **OS (OFFENSIVE SECURITY) ya que nos permite** ejecutar herramientas informáticas, principalmente aquellas enfocadas en ocasionar tropiezos en los diferentes sistemas informáticos, con el fin de conocer las diferentes falencias de seguridad que se puedan tener en nuestros sistema de información.

.

## 6.2 DESARROLLAR LA METODOLOGÍA DE HACKING ÉTICO SELECCIONADA AL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN DE LA ENTIDAD PIJAOS SALUD EPS INDIGENA SEDE IBAGUÉ, CON EL FIN DE IDENTIFICAR LAS VULNERABILIDADES Y AMENAZAS A LAS CUALES SE ENCUENTRA EXPUESTO.

### Fases de Trabajo e Implementación OS (OFFENSIVE SECURITY)

En las fases de desarrollo de la metodología escogida para este proyecto se realizó una planeación previa con el fin de dar seguimiento a cada etapa del proyecto, realizando una profunda identificación de los diferentes componentes del sistema de información de la entidad PIJAOS SALUD EPS INDIGENA sede Ibagué, tanto parte física como lógica buscando con esto una correcta obtención de resultados, aplicando como fuente inicial para la recolección de información una encuesta que permita por medio de cuestionarios dar respuesta a las diferentes preguntas que puedan surgir directa o indirectamente relacionadas con el caso de estudio,

buscando con esto poder implementar soluciones concretas que reduzcan y mitiguen las amenazas al sistema de información.

Como objetivo de esta metodología se tiene el poder determinar el estado actual de la seguridad del sistema de información de la EPS INDIGENA PIJAOS SALUD sede Ibagué, para esto se pretende emplear diferentes herramientas de seguridad informática de software libre que trabajan sobre LINUX. Este tipo de herramientas nos permitirán identificar más eficientemente las diferentes vulnerabilidades en los sistemas de información de la EPS INDIGENA PIJAOS SALUD sede Ibagué, inicialmente se tiene como muestra al personal que labora dentro de la sede de PIJAOS SALUD EPS. Los cuales participan activamente en las encuestas realizadas, las cuales se enfocan principalmente en la obtención del conocimiento que posee el personal de la EPS INDIGENA PIJAOS SALUD sede Ibagué, respecto a lo que es seguridad de la información, amenazas informáticas y vulnerabilidades del sistema. Todo esto enfatizando la importancia de tener ciertos conocimientos sobre el tema y con el objetivo principal de documentar por medio de estas encuestas que tan vulnerable se encuentra el sistema de información de la entidad y que tantos conocimientos tiene el personal que allí labora.

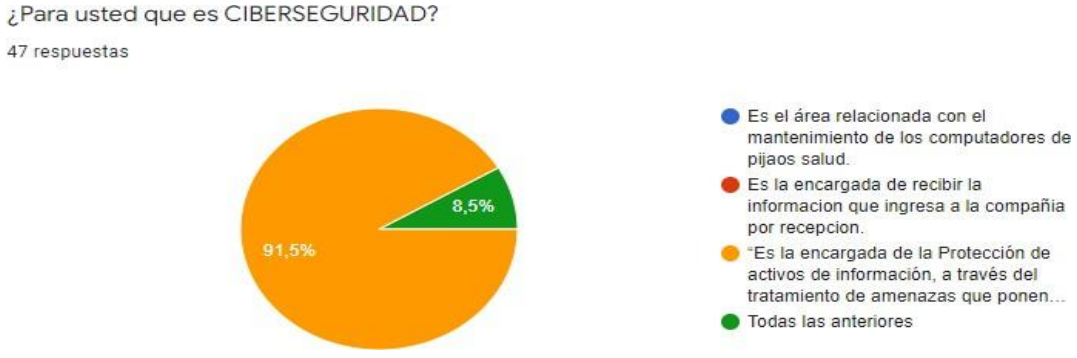
En el desarrollo de esta metodología seguiremos una serie de pasos para obtener los resultados esperados:

- Identificar con la ayuda de los funcionarios de la entidad y los usuarios responsables del sistema de información las falencias sobre la seguridad del sistema de información tomando como base la información recolectada en las diferentes encuestas realizadas.
- Identificar plenamente las políticas de seguridad y los manuales que rigen las mismas con el fin de conocer las posibles fallas que puedan ocasionar la aparición de amenazas al sistema de información.
- Establecer las herramientas de hacking ético, que serán utilizadas para la realización del análisis de vulnerabilidades y amenazas dentro de la red y en el sistema de información de la entidad.
- Implementar el uso de las herramientas establecidas para el análisis del sistema de información de la entidad con el fin de obtener los resultados de las posibles vulnerabilidades y amenazas dentro del sistema.
- Documentar de manera adecuada con el uso de los resultados presentados por el análisis las amenazas y vulnerabilidades encontradas dentro del sistema de información.
- Establecer los controles e implementar las políticas de seguridad de la información que hagan falta dentro de la entidad para corregir las falencias.

**Ilustración 3 Cuestionario Ciberseguridad**


Fuente: propia

**Ilustración 4 Pregunta 1**

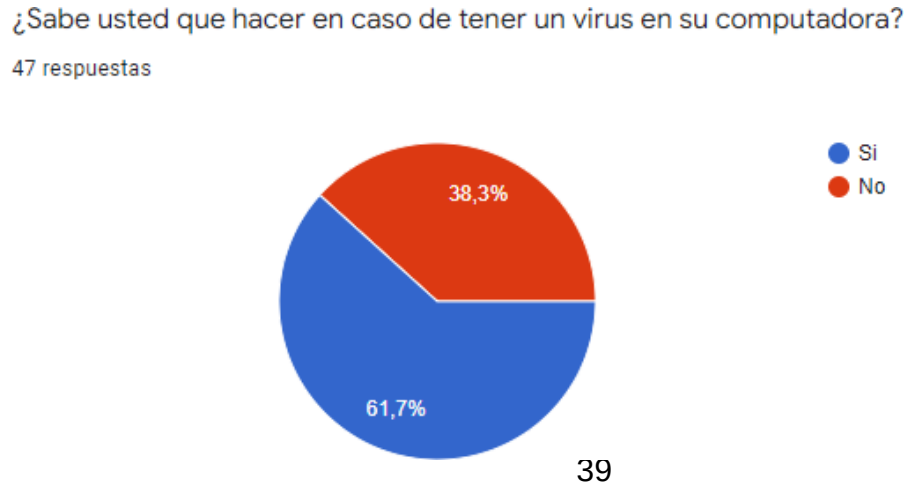


Fuente: propia

**Ilustración 5 Pregunta 2**

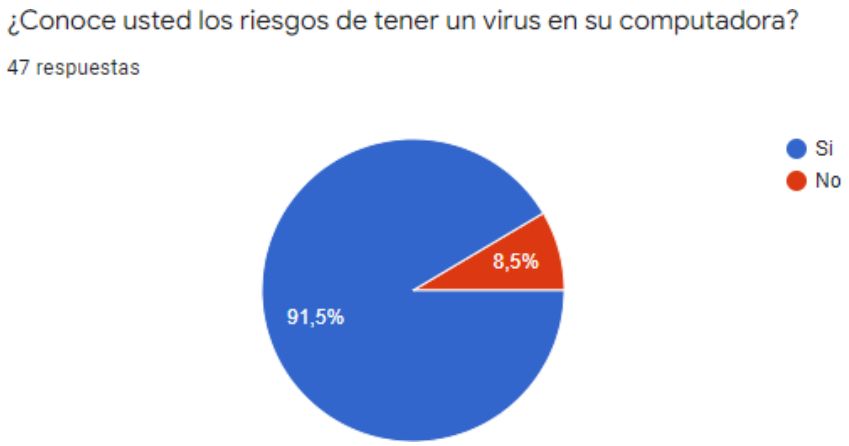

Fuente: propia

**Ilustración 6 Pregunta 3**



Fuente: propia

**Ilustración 7 Pregunta 4**

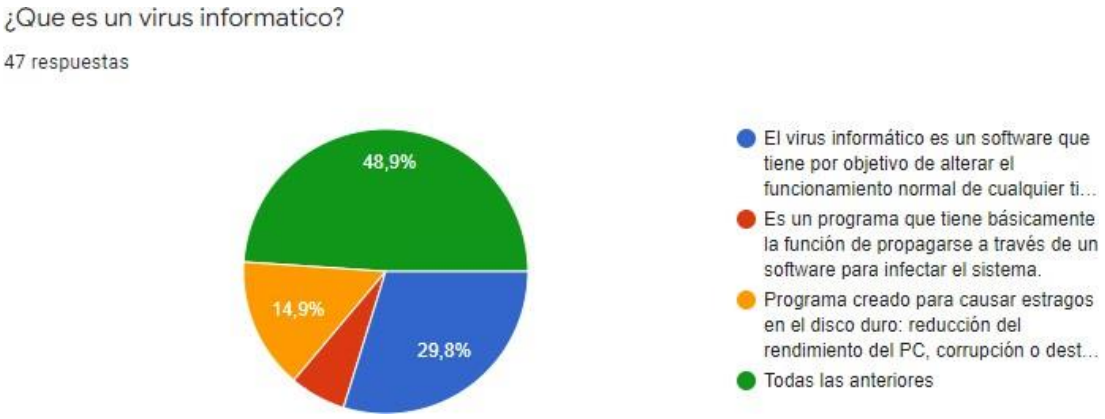



Fuente: propia

**Ilustración 8 Pregunta 5**

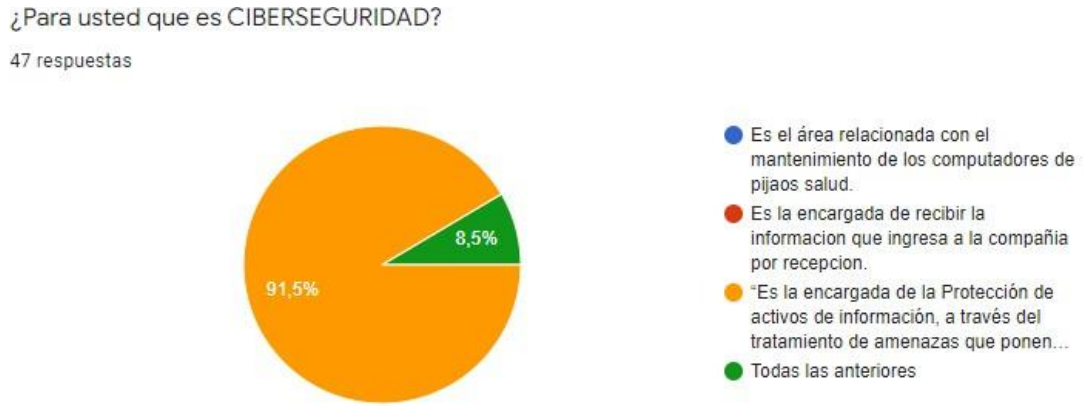
Fuente: propia

**Ilustración 9 Pregunta 6**




Fuente: propia

**Ilustración 10 Pregunta 7**



Fuente: propia

**Ilustración 11 Pregunta 8**


Fuente: propia

**POLITICAS DE SEGURIDAD DE LA EPS INDIGENA PIJAOS SALUD.**

Siguiendo las fases de la metodología se logra documentar que la entidad cuenta con un Manual de políticas de seguridad de la Información bien documentado el cual se encuentra versionado y actualizado cada año, o según las necesidades que surjan para su actualización, en el momento en que se inicia la documentación el manual se encontraba en la versión 2.2, pero por cambio de año y actualización que se trae a la fecha actual marzo de 2022 se realizó una actualización e inclusión de nuevas políticas al manual por demanda de la operación, poniendo el manual en su versión 2.3 actualmente.

**Ilustración 12 Caratula Manual de Políticas de Seguridad de la Información**

**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**

**PIJAOS SALUD EPS-I**

CODIGO: **EPSI-SYD-003**

Fuente: propia

**Cuadro 4 Versionado del Manual**

| | | | |
|---|---|---|---|
| | **POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN** | Código: | EPSI-SYD-003 |
| | | Versión: | 2.3 |
| | | Fecha: | 10/03/2022 |
| | Proceso: GESTION TICS SEGURIDAD DE LA INFORMACIÓN | Página: | 2 de 84 |

## 1 CONTROL DE VERSIONES

| Versión | Fecha Modificación | Comentario – Justificación |
|---|---|---|
| 1.0 | 01 febrero de 2018 | Versión Inicial |
| 2.0 | 01 octubre de 2019 | Actualización |
| 2.1 | 01 agosto de 2020 | Actualización |
| 2.2 | 01 febrero de 2021 | Actualización |
| 2.3 | 10 marzo de 2022 | Actualización |
| | | |

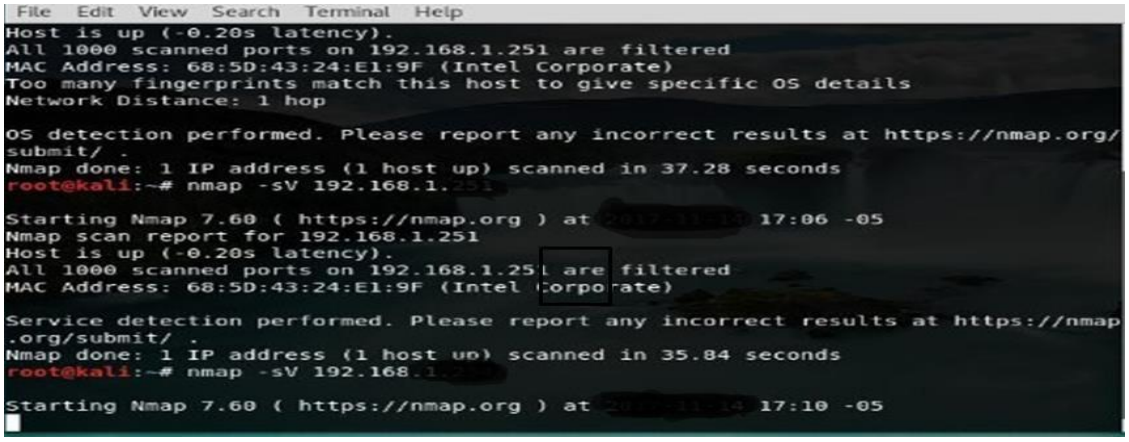
Fuente: propia

**Siguiente fase de aplicación de OS (OFFENSIVE SECURITY) intrusiones y hacking ético.**

Esta es la fase de información activa caracterizada por realizar directamente contacto con el objetivo propuesto en el proyecto, facilitando realizar las pruebas que sean necesarias en los servidores y demás sistemas de información a los que se está dirigido este proyecto, logrando simular el estado real en el que se encuentran los diferentes elementos del sistema, basando todo este estudio en las distintas herramientas a utilizar:

Se realizan **pruebas de penetración** con la ayuda de **Nmap**. Una herramienta de código abierto gratuita enfocada directamente en la exploración de la red y en la auditoria de seguridad de un sistema, esta herramienta se utilizara para realizar una exploración completa a la red informática que utiliza la EPS INDIGENA PIJAOS SALUD sede Ibagué, esto con el fin de dar un análisis más rápido a toda la red utilizando distintos paquetes IP para lograr determinar en tiempo real que servicios se encuentran activos en la red, que host están disponibles, corroborar también que sistema operativo utiliza la red y que versiona miento tiene, entre otra información que será de gran importancia para la documentación de amenazas y vulnerabilidades, información como que filtros de paquetes o qué tipo de cortafuegos están en uso entre otros datos de vital importancia para el caso de estudio.

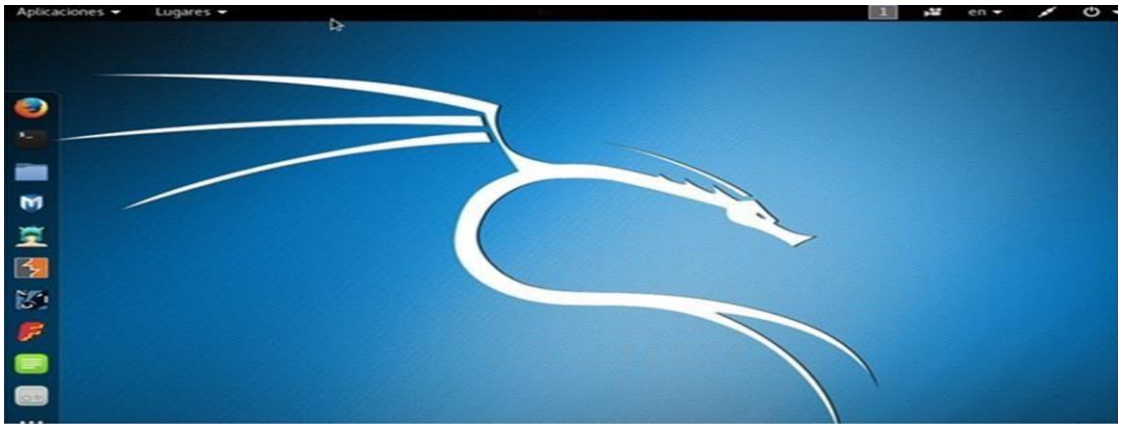
**Ilustración 13 Nmap**




Fuente: propia

Trabajando muy de la mano con las herramientas dispuestas por **Kali Linux** para la auditoria de sistemas de información las cuales permitirán conocer el estado real del sistema de información de la EPS INDIGENA PIJAOS SALUD sede Ibagué, brindándonos resultados integrales de los diferentes procesos a ejecutar, en busca de las diferentes vulnerabilidades y amenazas que pueda tener el sistema de información de la entidad, permitiéndonos con estos resultados encontrados adelantarnos a los posibles ataques que puedan derivar en pérdidas importantes de información para la entidad, traduciendo esto en una gran pérdida económica y de reputación, afectando todo el entorno laboral y comercial de la entidad.

**Ilustración 14 Kali Linux**

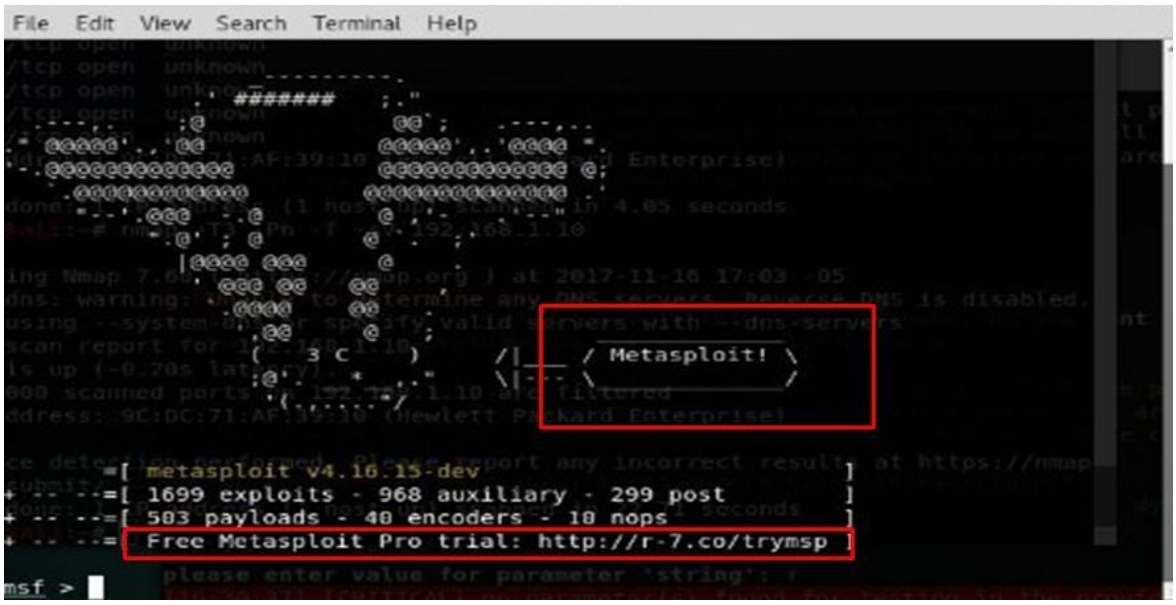



Fuente: propia

**Metasploit Framework** es otra importante herramienta que será utilizada en el desarrollo de la presente investigación para el desarrollo y ejecución de los diferentes exploits o ataques a las posibles vulnerabilidades de seguridad que pueda tener el sistema de información de la EPS INDIGENA PIJAOS SALUD sede Ibagué, esta herramienta se basa principalmente en tomar pedazos de código que intentan explotar una vulnerabilidad de seguridad definida. Se utiliza esta Herramienta con la finalidad de poder atacar las posibles vulnerabilidades del sistema de información. “La herramienta contiene más de 1500 exploits incluidos de forma predefinida, y se suele basar mucho en vulnerabilidades conocidas sobre versiones antiguas de un software determinado. Por ejemplo, tenemos la versión 7.0 de Apache Tomcat, de la que se detectó una vulnerabilidad de seguridad que fue corregida en la siguiente versión”[17]

**Ilustración 15 Meta Exploits**

[17] OPEN WEBINARS Hacking Tools: Herramientas para hacer pruebas de seguridad. [EN LÍNEA]. 23 agosto 2019. [Citado en 20 de noviembre de 2021]. Disponible en internet: < https://openwebinars.net/blog/hacking-tools/>

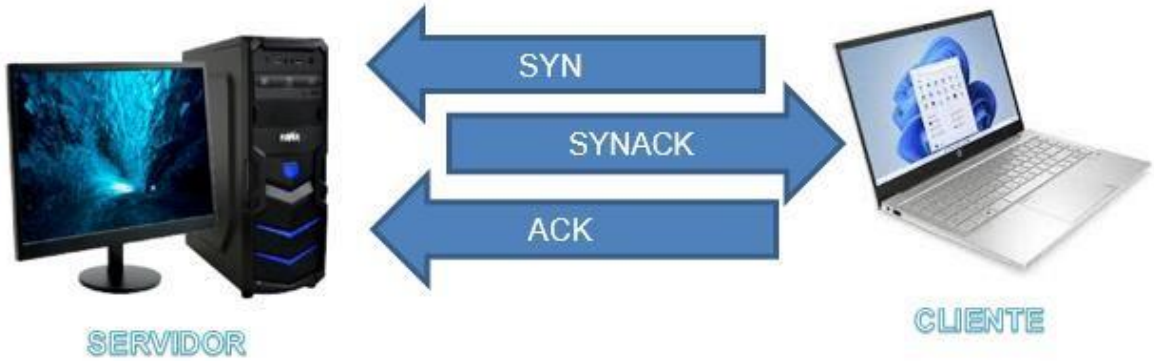



Fuente: propia

Se realiza escaneo a la red de la EPS INDIGENA PIJAOS SALUD sede Ibagué mediante la herramienta Nmap con la finalidad de encontrar puertos abiertos y vulnerabilidades de la red, se ejecutan una serie de comandos entre ellos

-sS sondeo TCP SYN: Este es un sondeo conocido como sondeo de abertura media ya que no llega a completar las conexiones TCP, con la negociación en 3 Pasos en el lado del servidor comprobamos si algún puerto está abierto si de pronto existe algún proceso corriendo en el mismo, pues se debe verificar que el destino tenga este servicio activo y este aceptando peticiones en el número de puerto al que estamos especificando o al rango si el puerto está cerrado se envía un RST, pero si se recibe un paquete SYNACK significa que el puerto si está abierto y con el fin de completar la negociación se envía de nuevo un ACK, entonces este escaneo con el comando –sS TCP SYN nos va a mostrar que puertos se encuentran abiertos y recibiendo paquetes.

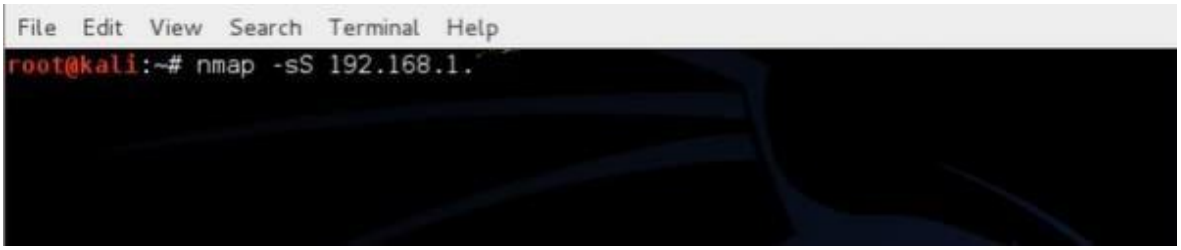
**Ilustración 16 Escaneo -sS TCP SYN**



Fuente: propia

Se corre el comando –sS para conocer específicamente que puertos se encuentran abiertos y están disponibles para él envió de paquetes. Se realiza este escaneo al servidor de la EPS INDIGENA referenciando todos los puertos activos y abiertos.

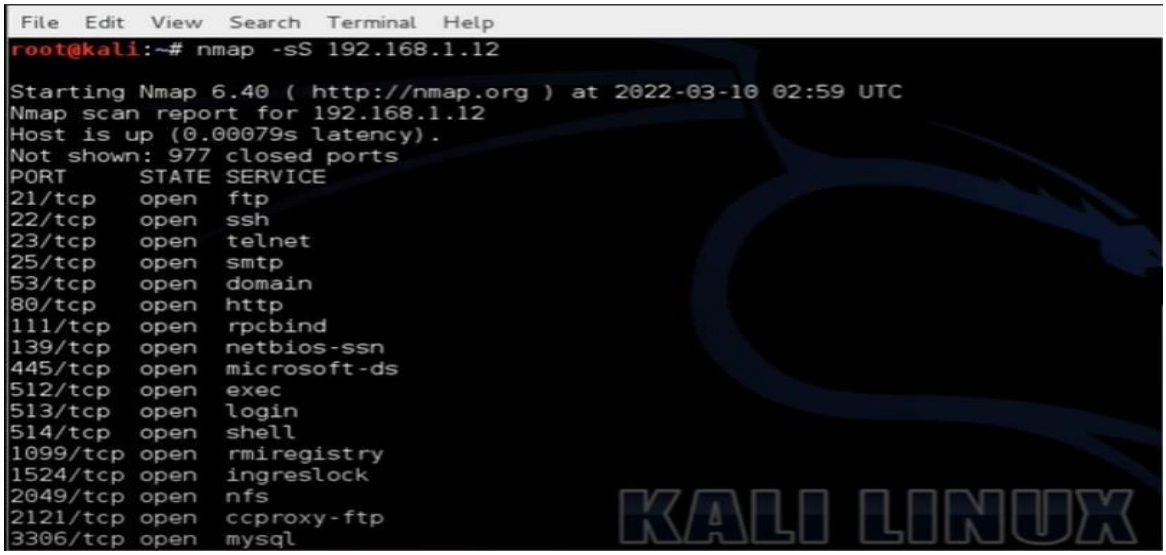
**Ilustración 17 Comando –sS**




Fuente: propia

Una vez se corre el escaneo con el comando –sS nos arroja el resultado de los puertos que se encuentran abiertos en el servidor de la EPS INDIGENA, esta es información bastante útil para poder controlar los diferentes puertos de nuestro servidor verificado cuales se encuentran abiertos y cuáles no dándonos el conocimiento básico de nuestra red interna, información útil para mantener un control adecuado de la seguridad de nuestra red.

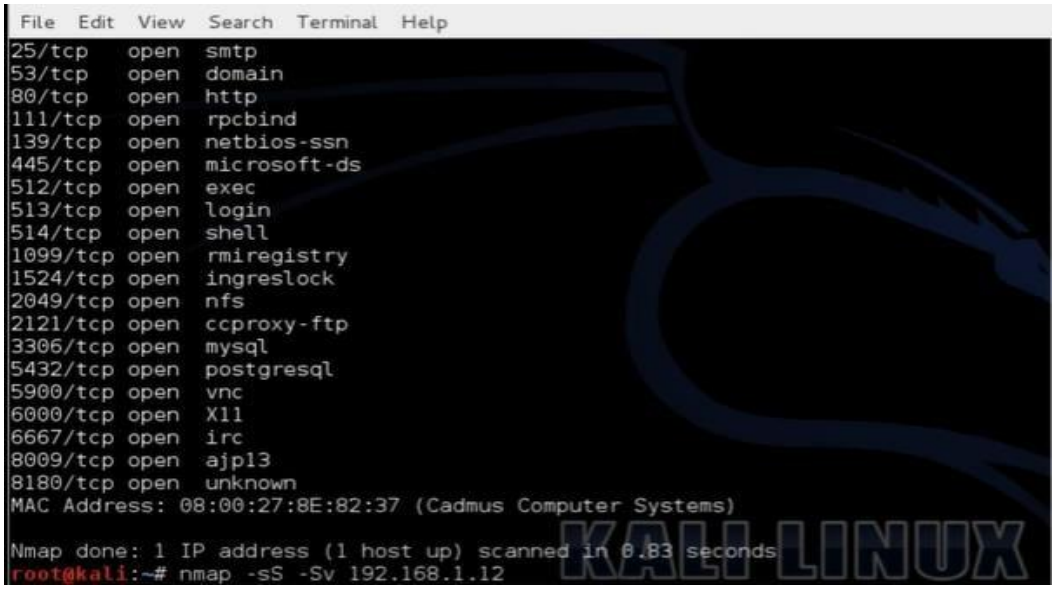
**Ilustración 18 Resultado del Escaneo -sS**




Fuente: propia

Podemos utilizar también el comando –sS –sV con el que podremos identificar qué y cuáles son las versiones de los servicios que están corriendo por estos puertos, esto permitiéndonos ver qué servicios se encuentran vulnerables y como poder mitigar dichas vulnerabilidades confirmando las versiones de software que se encuentran en estos servicios.

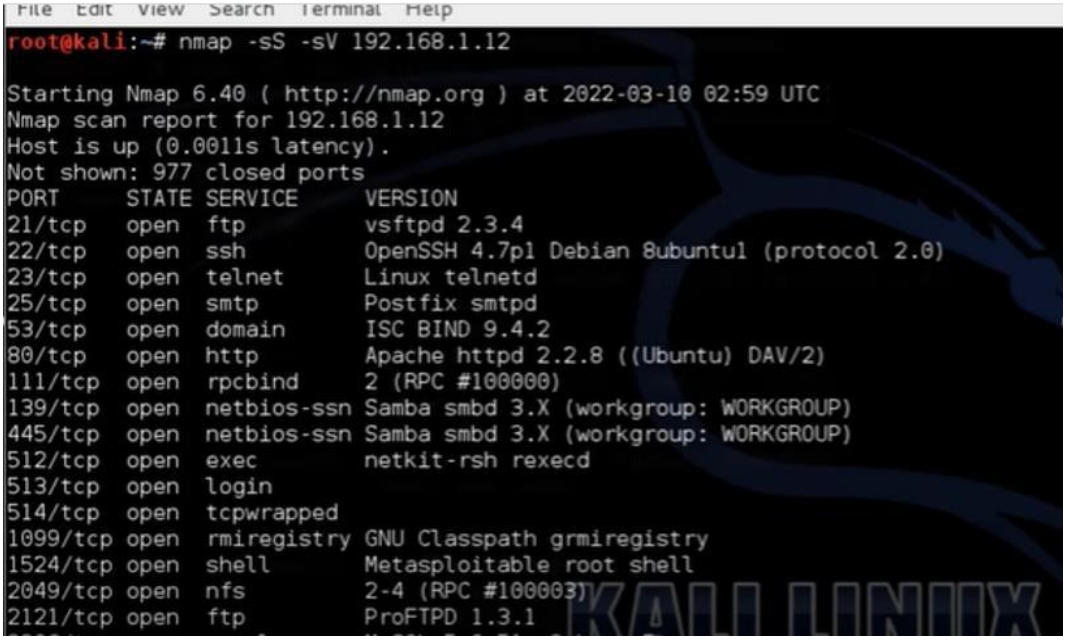
**Ilustración 19 Comando -sS -sV**




Fuente: propia

Una vez se realiza el escaneo podemos identificar que el versionado de algunos de los servicios que se encuentran corriendo actualmente sobre los puertos del servidor de la EPS INDIGENA se encuentran sin su debida actualización haciendo que esto se convierta en una vulnerabilidad para la seguridad y una amenaza para el sistema de información de esta  entidad.

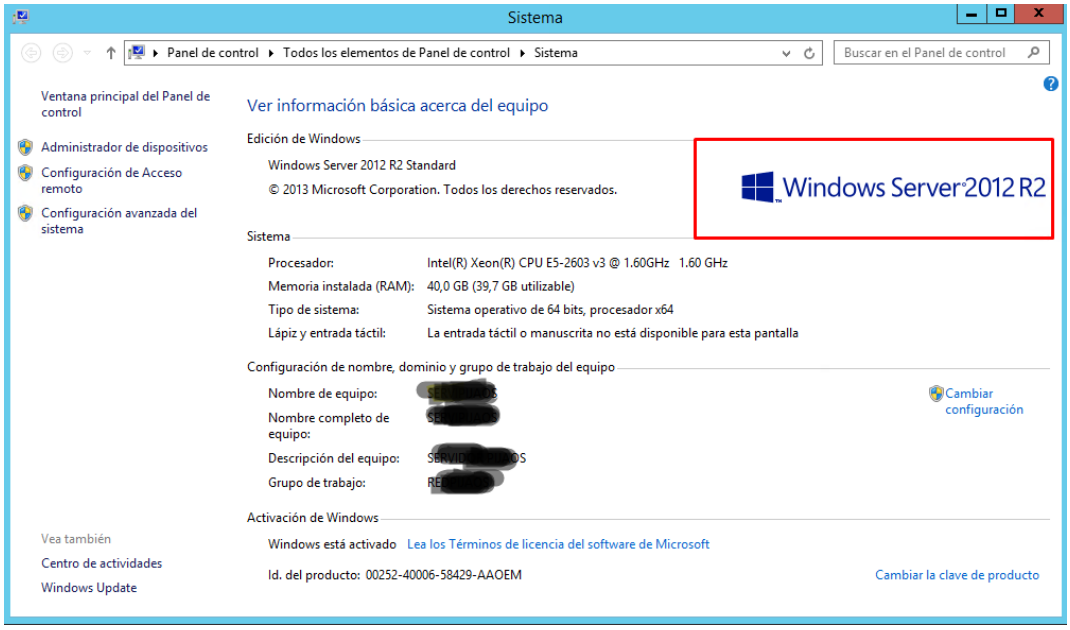
**Ilustración 20 Resultado Comando -sS -sV**



Fuente: propia

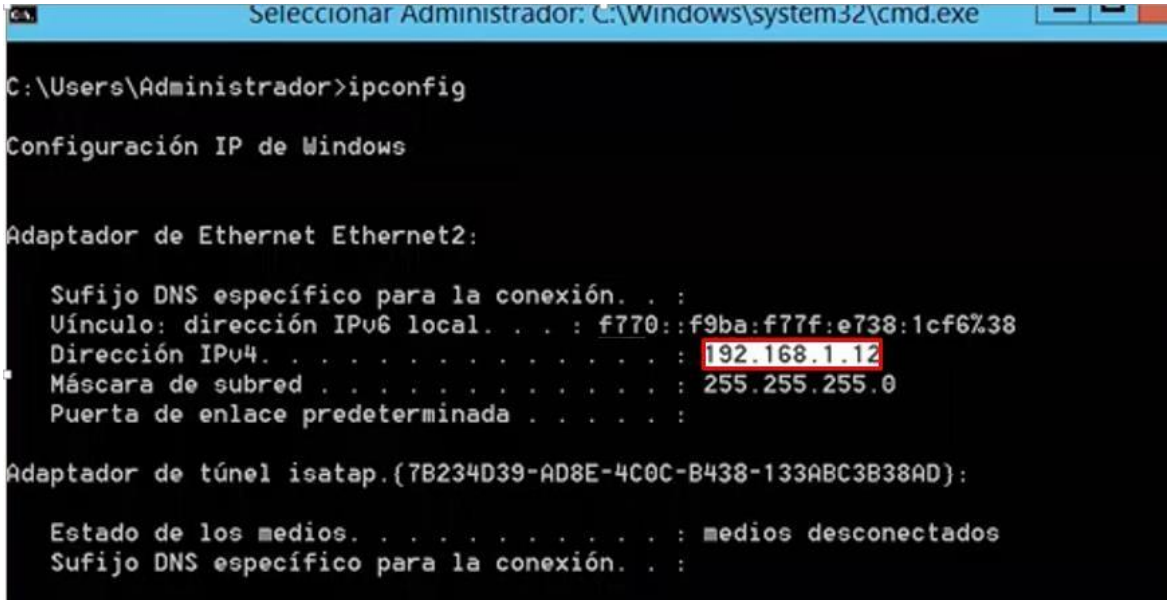
**Metasploit Vulneración del servidor WINDOWS SERVER 2012 R** Se realiza un intento de vulnerar el servidor que es usado por la EPS INDIGENA PIJAOS SALUD sede Ibagué para el manejo de su información y plataformas institucionales. Este intento se realiza por medio de Metasploit y se realiza principalmente con la finalidad de conocer las vulnerabilidades que existen actualmente y poder con esta información tomar decisiones de valor en cuanto a cómo se va a realizar la gestión de defensa frente a esta.

**Ilustración 21 Servidor Windows Server 2012 R2**



Fuente: propia

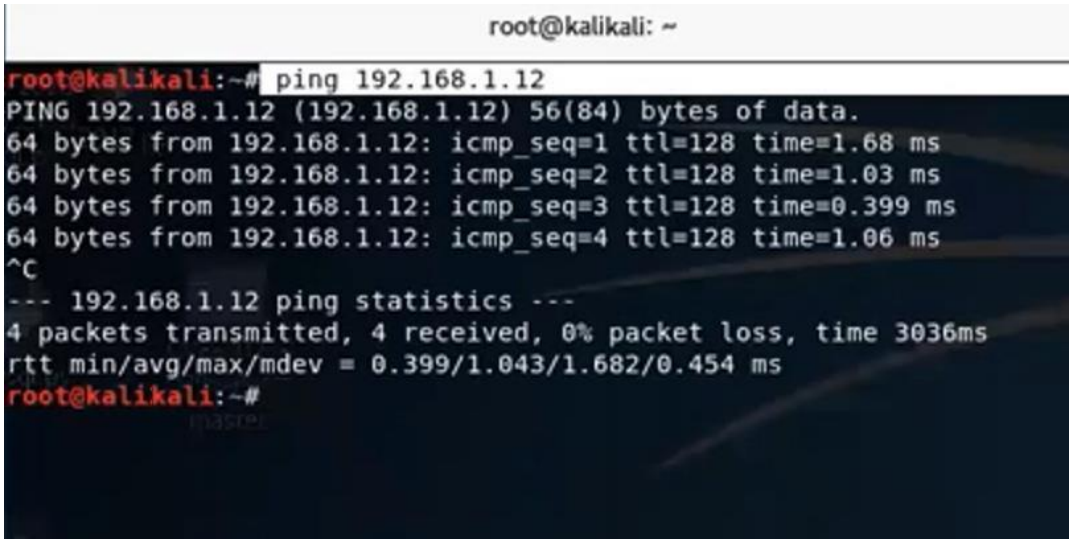
**Ilustración 22 IP Servidor**




Fuente: propia

Una vez tenemos sabemos cuál es la IP del servidor destino del ataque debemos realizar ping de respuestas para verificar su disponibilidad en la red.

**Ilustración 23 Ping al Servidor**

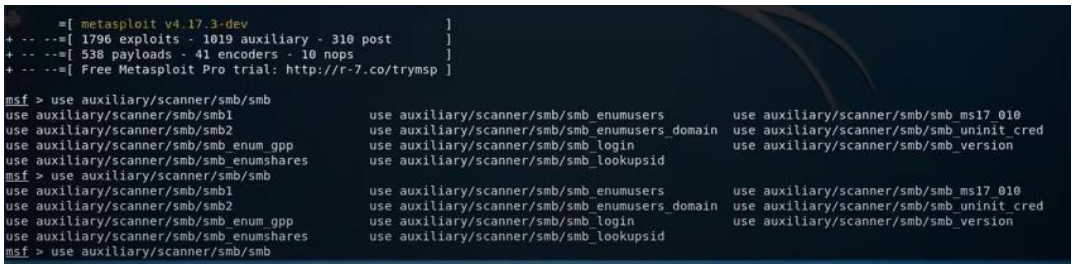



Fuente: propia

Teniendo claro que el servidor se encuentra disponible en la red procedemos a iniciar el trabajo con la herramienta Metasploit enfocando el ataque directamente a la IP del servidor, utilizando para este ataque un auxiliar que realizara el escaneo a la víctima. Con el comando

*.> use auxiliary/scanner/smb/smb_ms17_010*

**Ilustración 24 Inicio de trabajo con Metasploit**

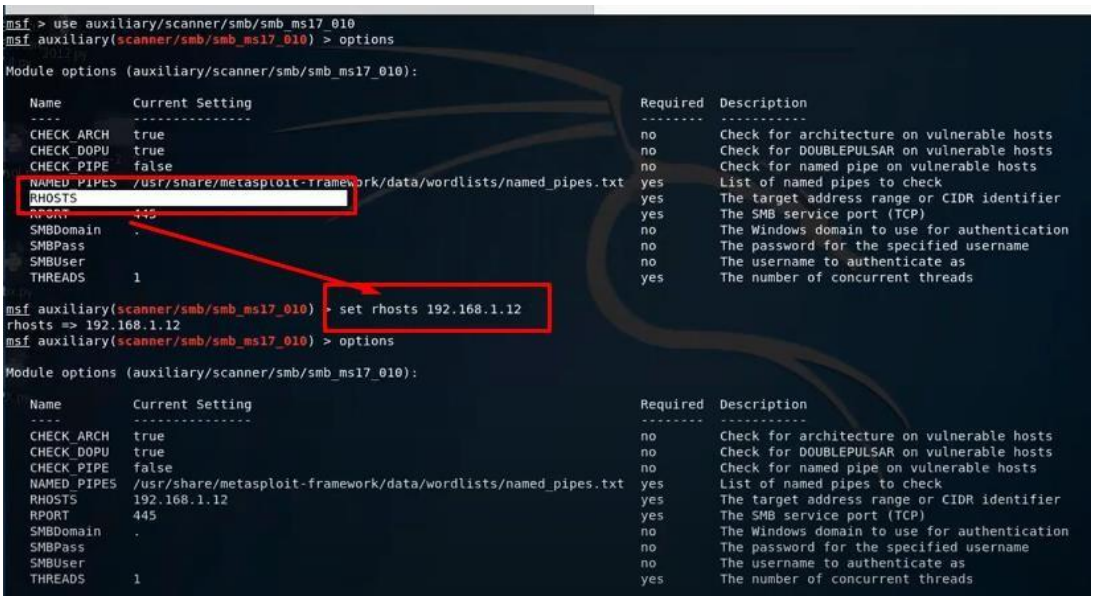



Fuente: propia

Una vez iniciamos el trabajo con la herramienta empezamos a realizar el escaneo a la víctima (Servidor) realizamos un set a la IP del Servidor para poder enfocar el ataque directamente a la IP correcta trabajando un Run al escáner con los comandos

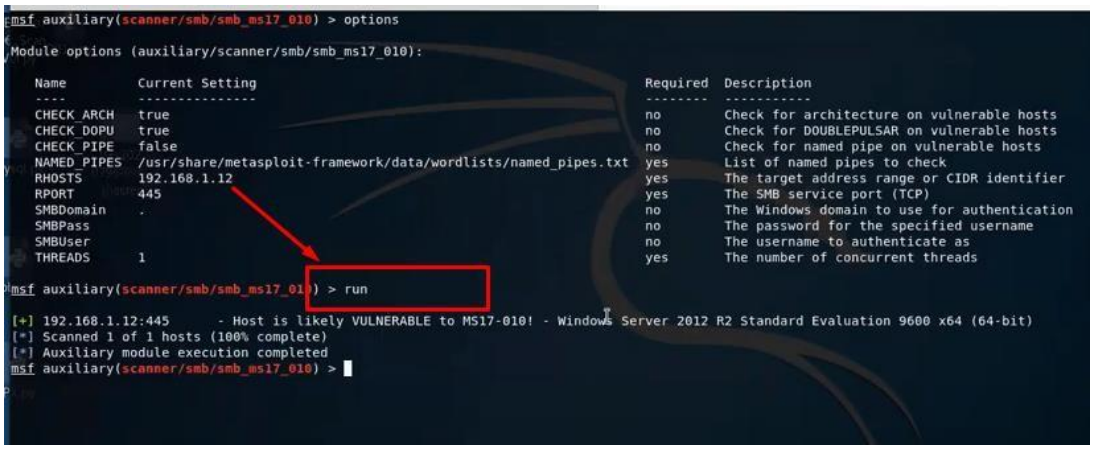
*.> set rhosts 192.168.1.***

**Ilustración 25 set a IP del Server**




Fuente: propia

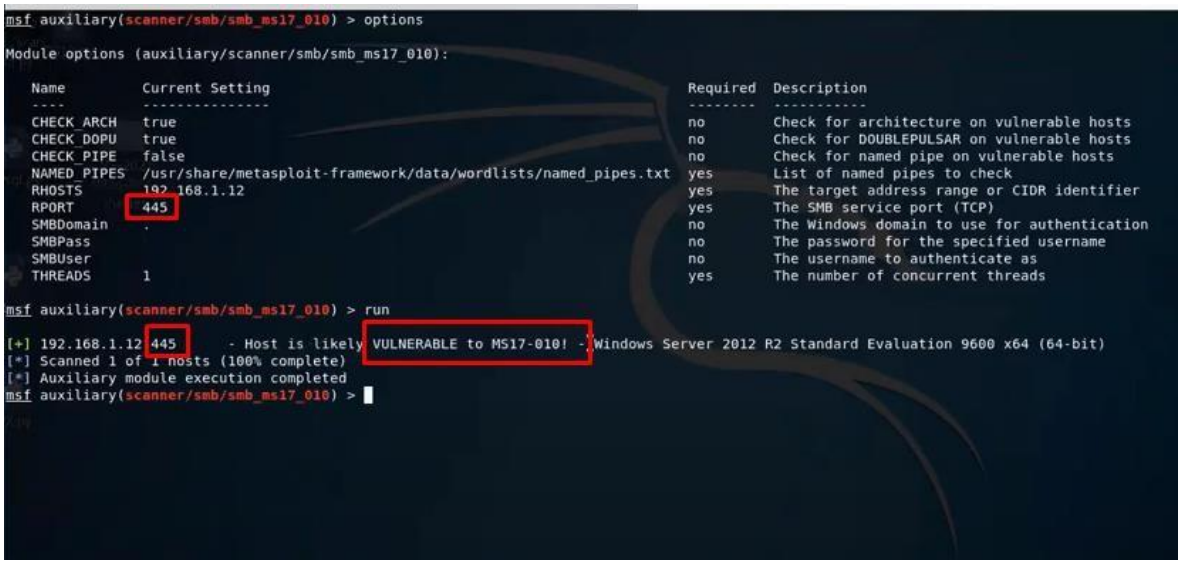
**Ilustración 26 Corremos el Escaneo a la IP del Server**




Fuente: propia

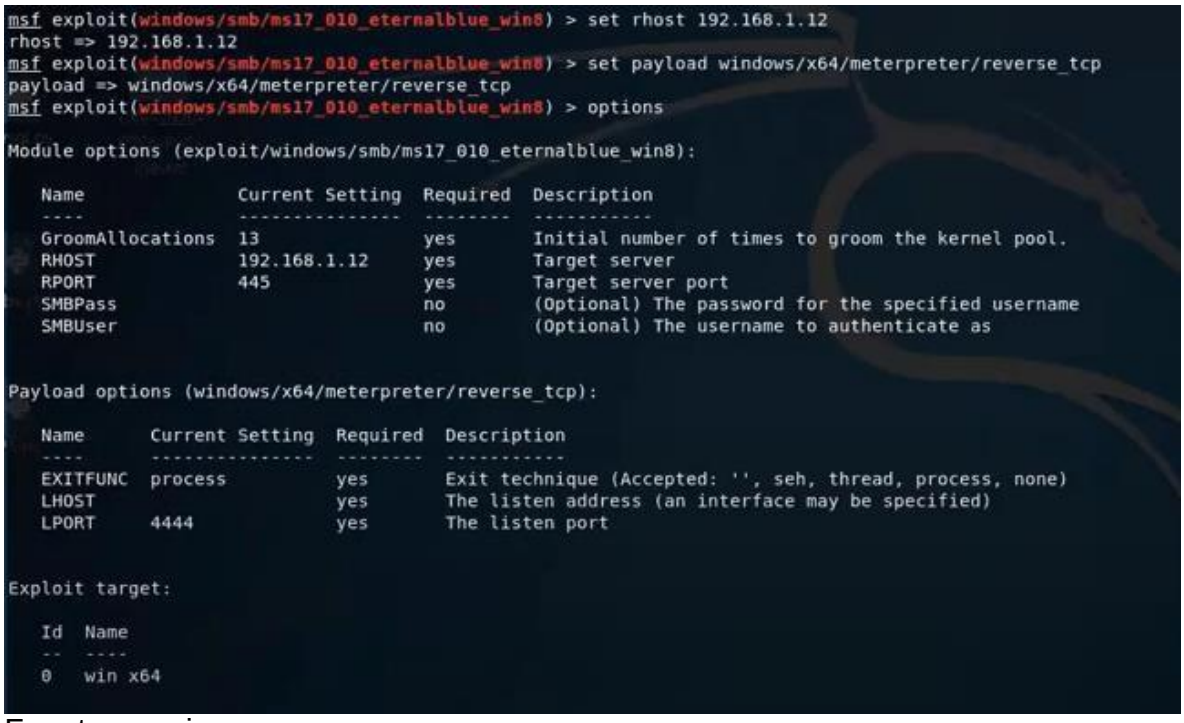
Una vez se realizó el escaneo del servidor de la EPSI INDIGENA PIJAOS SALUD sede Ibagué nos podemos dar cuenta que presenta una vulnerabilidad to MS17 – 010 Esta es una vulnerabilidad que da como resultado exitoso después de ser explotada el lograr la ejecución de forma remota del código de cualquier computadora o servidor que se tenga como destino permitiendo, dando la oportunidad a un atacante de cargar algún código malicioso (malware) logrando contaminar toda una red por medio de los host que se encuentran vulnerables en esta red así como se muestra en la siguiente ilustración.

**Ilustración 27 Vulnerabilidad Encontrada**



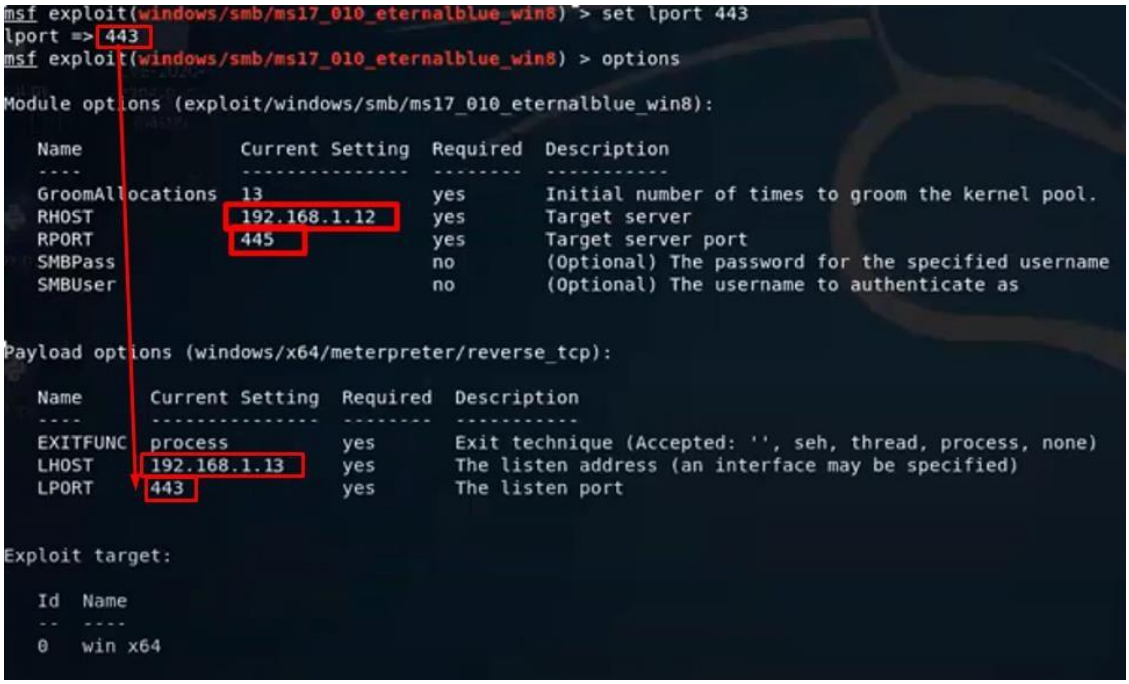

Fuente: propia

**Ilustración 28 Uso de la Vulnerabilidad**




Fuente: propia

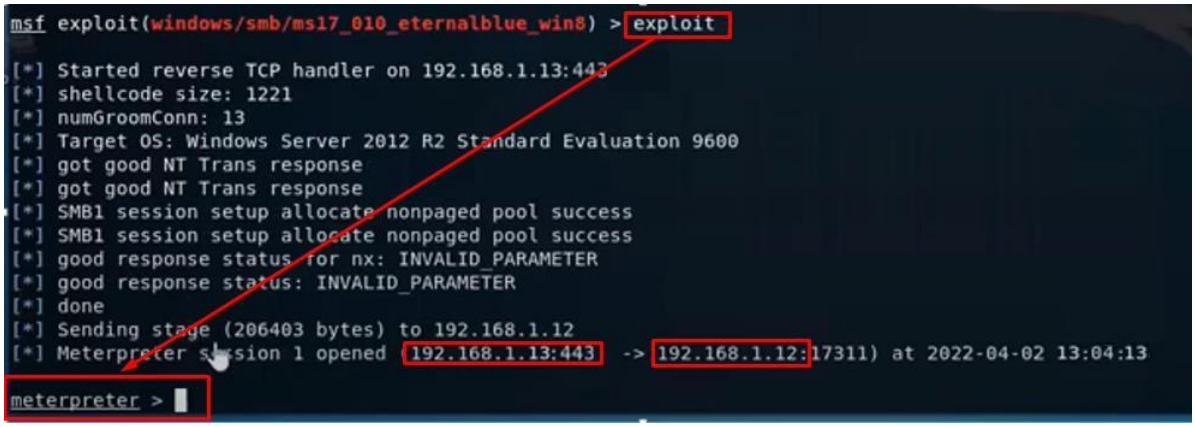
**Ilustración 29 Cambio de Puerto**




Fuente: propia

Luego de seguir los pasos con los comandos y correctos podremos demostrar por medio del siguiente procedimiento que si es posible vulnerar el servidor de la EPS INDIGENA PIJAOS SALUD sede Ibagué, logrando tomar control de forma remota del servidor por medio del **Meterpreter**, un programa troyano que resulta siendo malicioso y nos da el control de forma remota del servidor. Infectándolo y ejecutando el malware en la memoria del servidor sin necesidad de escribir absolutamente nada en el disco, siendo así indetectable para los ojos de los usuarios normales ya que no se crea ningún proceso nuevo.

**Ilustración 30 Ataque Finalizado**




Fuente: propia

## 6.3 DISEÑAR UN INFORME QUE RELACIONES LOS CONTROLES QUE PERMITAN MITIGAR EL RIESGO ASOCIADO A LAS VULNERABILIDADES IDENTIFICADAS PARA UNA CORRECTA GESTIÓN DE CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN DE LA ORGANIZACIÓN.

Se diseña un informe que se presenta a la gerencia de Pijaos salud EPS Indígena y a las directivas de la entidad dando a conocer alternativas de seguridad que son necesarias Enfocando la búsqueda de alternativas en los resultados del análisis que se realizó mediante las diferentes pruebas y procesos de la metodología de hacking ético y pen test utilizadas y que nos mostraron diferentes vulnerabilidades de seguridad halladas en el sistema de información de Pijaos salud EPS Indígena Sede Ibagué.

La falta de un producto que pueda suplir la necesidad de seguridad y que proteja el activo más valioso de la entidad, se convierte en el problema más grande que se tiene debido a que el mundo informático este día a día cambiando y generando nuevas amenazas que pueden llegar a ser tan perjudiciales para cualquier entidad. Dicha situación tiene en riesgo el correcto funcionamiento y productividad de la entidad, ya que se nos presentan diferentes factores que afectan la continuidad de la operación y que siguen interrumpiendo la toma de decisiones y que además provocan perdidas de información y tiempo convirtiéndose en una gran pérdida de recursos económicos.

Se anexa informe con alternativas de solución presentadas a las directivas de la entidad, después de una búsqueda de proveedores del servicio de seguridad informática en vista que en este momento PIJAOS SALUD se encuentra vulnerable ante un ataque informático, existe una necesidad de adquirir un paquete de Ciberseguridad más robusto para las necesidades que tiene la EPSI con un proveedor que brinde las garantías necesarias de calidad, conectividad, soporte y de una herramienta tecnológica moderna la cual proporcionará una mayor flexibilidad y mejor accesibilidad a la información y manejo de la operación.

# 7 CONCLUSIONES

PIJAOS SALUD EPSI es una entidad que no cuenta con las herramientas suficientes para lograr mantener una seguridad media de su información, es importante que se tenga presente que las vulnerabilidades encontradas son reflejo del estado real de su sistema de información y genera un peligro latente para su confidencialidad, integridad y disponibilidad, haciendo importante el poder contar con firewall que permitan mitigar distintas vulnerabilidades y gestionar los riesgos asociados. Generando también unas políticas de seguridad de la información más robustas que busquen la mitigación de riesgos y el control de accesos no autorizados a sus sistemas, trabajando de la mano de capacitaciones constantes a sus funcionarios ya que después de involucrar diferentes metodologías y procedimientos de hacking Ético, como lo son la realización de encuestas a los funcionarios de Pijaos Salud EPS Indígena sede Ibagué, se toma como resultado la falta de capacitación y de conocimiento de los funcionarios sobre temas de seguridad informática dentro de la entidad, es por esta razón que se hace de suma importancia el poder tener estudios como el que se realizó con metodologías de hacking ético y pen test dentro de la entidad.

Teniendo en cuenta las características y funcionalidades contempladas en cada metodología de hacking ético es importante determinar cuál es la metodología más adecuada, que pueda dar continuidad al correcto desarrollo del análisis y posterior solución a las problemáticas halladas, no obstante es importante también mencionar que gracias al análisis que se desarrolló con la ayuda de diferentes herramientas utilizadas en este estudio para las pruebas de penetración que se realizaron, se logró determinar el estado real de la seguridad de la información dentro de la EPS Indígena. Con herramientas como Kali Linux y sus diferentes funcionalidades al igual que Nmap entre otras.

Utilizando estas diferentes herramientas se logró identificar la falta de capacitación al personal encargado de la seguridad de la información dentro de la entidad, además de las falencias que presentan en el servidor debido a que no se tiene un control adecuado en el acceso a dichos elementos. De la misma manera gracias a las pruebas realizadas se logra identificar algunos de los puertos que se encuentran abiertos y que exponen la integridad y confidencialidad de la información que reposa en el servidor de la entidad, esto se logró determinar con la ayuda de las herramientas de hacking ético mencionadas anteriormente, generando una alerta temprana a la seguridad del sistema de información de la entidad, concluyendo que se necesita de manera inmediata se tome en cuenta la implementación de nuevas medidas de seguridad para el resguardo de sus servidores y los puertos que están quedando expuestos, ya que se logró comprobar un acceso por medio de técnicas de hacking ético y que preocupan al resultado de este estudio, recordando la

importancia de tomar en cuenta el presente estudio para generar las medidas necesarias que permitan asegurar de una manera más eficaz la seguridad de la información dentro de la entidad, implementando los controles necesarios que procuren mitigar el riesgo latente que enfrentan los sistemas de información de la entidad.

Concluyendo con el informe presentado a la gerencia de la EPSI que se debe poner mucha atención a los resultados del estudio, ya que estos reflejan el estado real del sistema de información la falta de seguridad de sus diferentes bases de datos y demás información que reposan en sus servidores.

# 8 RECOMENDACIONES

Una vez realizado el estudio, es importante resaltar que se tienen algunas recomendaciones que se basan primordialmente en aquellos aspectos encontrados en los procedimientos que se llevaron a cabo y que serán mencionadas a continuación:

- Se recomienda el poder tener implementado dentro de la entidad una planeación más elaborada sobre los mantenimientos preventivos a los diferentes equipos de cómputo que tengan injerencia directa sobre el sistema de información de la EPS Indígena, esto referenciado por la metodología **OS (OFFENSIVE SECURITY)** establecida para el presente estudio con la finalidad de tener un control de vulnerabilidades realizando pruebas de manera regular a sus sistemas de información.

- Establecer unas políticas de seguridad de la información donde se pueda contemplar la realización de diferentes pruebas de penetración por medio de la metodología **OS (OFFENSIVE SECURITY)** teniendo en cuenta la importancia de detectar falencias y vulnerabilidades a tiempo.

- Se recomienda implementar un proceso interno que sea el encargado de gestionar directamente la capacitación del personal involucrado en la seguridad de la información dentro de la entidad con el fin de actualizar conocimientos y evitar futuras intrusiones de terceros al sistema de información de la EPS Indígena. Ya que en las diferentes pruebas de penetración realizadas en el presente estudio se detectaron algunas falencias en sus sistemas de información.

- Es de suma importancia el poder implementar dentro de las políticas de seguridad de la entidad un control de acceso de los usuarios más efectivo que pueda tener un verdadero control de la información que ingresa y también de la información que se extrae de las bases de datos de la entidad, teniendo como referente la falta de controles y la poca información que los empleados de la entidad tiene sobre el tema, tomando como base los resultados del test de conocimiento realizado al personal.

- Se recomienda de igual manera en las políticas de seguridad de la información pueda ser implementada una política de creación de backups de las bases de datos que se gestionan teniendo como referente que se encuentran una serie de falencias en los sistemas de seguridad de

información de la entidad y puede llegar a presentarse perdidas de sus bases de datos eventualmente.

- Los Encargados de los activos de información deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos o áreas.

- Periódicamente, El área encargada de Seguridad de la Información de la EPSI debe efectuar la revisión de los programas utilizados en cada equipo. La descarga, instalación o uso de aplicativos o programas informáticos NO autorizados debe ser considerada como una violación a las Políticas de Seguridad de la Información de PIJAOS SALUD EPSI.

- En la entidad Pijaos Salud EPS Indígena se debe suministrar a cada usuario las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, estas claves deben ser de uso personal e intransferible y deber ser de responsabilidad del usuario el manejo apropiado a las claves asignadas para el ingreso al sistema de información.

- Se recomienda que el área de Seguridad de la Información, a través de sus funcionarios, debe asegurarse que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware con el fin de que no pueda ser ejecutado ningún programa malicioso dentro del servidor de la entidad.

# 9 BIBLIOGRAFÍA


BAUTISTA GARCIA, Ivan. Hacking ético: ¿en qué consiste y por qué es importante? [EN LÍNEA].2020. [Citado en 09 de octubre de 2021]. Disponible en internet: < https://www.servnet.mx/blog/hacking-etico-en-que-consiste-y-por-que-es-importante>

CARDENAS, Fabián. ¿Qué es la gestión de activos de información?. [EN LÍNEA].2020. [Citado en 09 de octubre de 2021]. Disponible en internet: < https://www.novasec.co/blog/67-gestion-de-activos-de-informacion/>

COMUNICACIONES, M. d. (s.f.). MINTIC - Todos por un nuevo país. Obtenido de http://www.mintic.gov.co/

COLOMBIA. MINISTERIO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Fortalecimiento de las TI de la información en la gestión del Estado y la información pública [en línea]. [Citado 10 de octubre de 2021]. Disponible en Internet en: <http://www.mintic.gov.co/portal/vivedigital/612/w3- propertyvalue-657.html>

Controles de Seguridad y Privacidad de la Información. [En línea]. <https://www.mintic.gov.co/gestionti/615/articles- 5482_G8_Controles_Seguridad.pdf>

DIGITAL GUIDE, Ethical hacking: solucionar fallos de seguridad y prevenir la cibercriminalidad. [EN LÍNEA].06 noviembre 2020. [Citado en 09 de octubre de 2021]. Disponible en internet: <https://www.ionos.es/digitalguide/servidores/seguridad/que-es-el-ethical-hacking/>

FERNÁNDEZ, E. Metodología para el diseño de bases de datos seguras. La Mancha: Universidad de Castilla, 2002.

FICARRA, Francisco. “Los virus informáticos: Entre el negocio y el temor”. Revista Latinoamericana de Comunicación CHASQUI. [En línea]. Junio 2002. [09 octubre de 2021]. Disponible en: <http://www.redalyc.org/articulo.oa?id=16007810.>

Guía para la Implementación de Seguridad de la Información en una MIPYME. [En línea]. Bogotá: MINTIC. 2016., 31 p. Disponible en: <https://www.mintic.gov.co/gestionti/615/articles5482_Guia_Seguridad_informacion_Mypimes.pdf.>

HERALDO.“10 consejos para prevenir un ataque informático” [en línea], marzo 2015 [consultado el 10 octubre de 2021]. Disponible en Internet: < http://www.heraldo.es/noticias/comunicacion/2015/03/31/diez_consejos_para_prevenir_ataque_informatico_348654_311.html>.

HUILCA, Gloria Nataly, Tesis_t764si.pdf - Repositorio Universidad Técnica de Ambato. [EN LÍNEA].22 noviembre 2012. [Citado en 22 de abril de 2021]. Disponible en internet: <https://repositorio.uta.edu.ec/bitstream/123456789/2900/1/Tesis_t764si.pdf

Infolaft, Anticorrupción, fraude y LA/FT, ¿Qué hacer antes, durante y después de un ataque informático? [EN LÍNEA]. 2021. [Citado en 08 de octubre de 2021]. Disponible en internet: < https://www.infolaft.com/que-hacer-antes-durante-y-despues-de-un-ataque-informatico/>

INTECO. Política de contraseñas y seguridad de la información. [En línea]. Bogotá: Instituto Nacional de Tecnologías de la Comunicación. 2017., 7 p. Disponible en: <https://www.unirioja.es/servicios/si/seguridad/difusion/politica_contrasenas.pdf>

ISO 27001, La Seguridad de la Información en la Gestión de la Continuidad de Negocio. [En línea]. [Citado en 08 de octubre de 2021]. Disponible en internet: <http://www.pmg-ssi.com/2014/11/iso-27001-la-seguridad-de- la-información-en-la-gestión-de-la-continuidad-de-negocio/>

LIA, Solutions SAS. Seguridad Informática. [EN LÍNEA]. 2021. [Citado en 08 de octubre de 2021]. Disponible en internet: < https://www.liacolombia.com/seguridad-informatica>

LR, LA REPUBLICA, Colombia ocupa el puesto 39 en el ranking mundial sobre ciberseguridad. [EN LÍNEA]. 02 junio 2020. [Citado en 08 de octubre de 2021]. Disponible en internet: < https://www.larepublica.co/globoeconomia/ciberseguridad-otro-reto-que-deben-enfrentar-las-empresas-en-el-mundo-por-covid-3013083>

MANUAL Estrategia de Gobierno en Línea. Disponible en (http://estrategia.gobiernoenlinea.gov.co/623/articles-7941_manualGEL.pdf)

MÉNDEZ, C. Metodología de la investigación para ciencias empresariales. Bogotá: Mc Graw Hill, 2003.

MINTIC. Seguridad y Privacidad de la Información. [EN LÍNEA].2016. [Citado en 09 de octubre de 2021]. Disponible en internet: < https://mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf/>

MOJICA, M. Implementación y administración del sistema de información del Ministerio de Educación Nacional SICIED (sistema interactivo de consulta de infraestructura educativa). Trabajo de Grado. Ingeniero de Sistemas. San José de Cúcuta: Universidad Francisco de Paula Santander. Facultad de Ingeniería. Departamento de Ingeniería de Sistemas, 2011. Monroy, Sergio. Protección de datos en hospitales: Políticas de seguridad informática. [EN LÍNEA]. 26 junio 2019. [Citado en 08 de octubre de 2021]. Disponible en internet: < https://dondoctor.com/sector-salud-colombia/proteccion-de-datos-en-hospitales-10-politicas-de-seguridad-informatica/>

NUESTRA IDENTIDAD DIGITAL ¿A qué se denomina Riesgo Informático? [EN LÍNEA].2020. [Citado en 09 de octubre de 2021]. Disponible en internet:https://sites.google.com/site/nuestraidentidaddigital/riesgos-informaticos/

OPEN WEBINARS Hacking Tools: Herramientas para hacer pruebas de seguridad. [EN LÍNEA]. 23 agosto 2019. [Citado en 20 de noviembre de 2021]. Disponible en internet: < https://openwebinars.net/blog/hacking-tools/>

ORGANIZACIÓN INTERNACIONAL DE ESTANDARIZACIÓN. Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información. ISO/IEC 17799:2005. Bogotá: ISO.

ORTIZ, Ángel. ¿Qué es una amenaza informática? ¿Cómo contenerla? [EN LÍNEA].2020. [Citado en 09 de octubre de 2021]. Disponible en internet: < https://www.hostdime.la/blog/que-es-una-amenaza-informatica-como-contenerla/>

ORTIZ, Ángel. ¿Qué es una vulnerabilidad en seguridad informática? [EN LÍNEA].2020. [Citado en 09 de octubre de 2021]. Disponible en internet: < https://www.hostdime.com.pe/blog/que-es-una-vulnerabilidad-en-seguridad-informatica-ejemplos/>

PÉREZ, M. (2012). Módulo 3: auditorías y seguridad. Tema 4: comparativa metodologías auditorías y pentesting. Elche: Campus Virtual.

PROFITLINE, Actualmente Como se encuentra Colombia en Seguridad Informática. [EN LÍNEA].26 febrero 2019. [Citado en 09 de octubre de 2021]. Disponible en internet: < https://profitline.com.co/actualmente-como-se-encuentra-colombia-en-seguridad-informatica/ >

RSS ENTRIES. Gestión de Riesgo en la Seguridad Informática 101 [en línea]. [Consultado 12 de octubre de 2021]. Disponible en Internet en: https://protejete.wordpress.com/glosario/

SEGURIDAD INFORMATICA. Objetivos de la seguridad informática [EN LÍNEA].2020. [Citado en 09 de octubre de 2021]. Disponible en internet: < https://infosegur.wordpress.com/tag/confidencialidad/>

SORIANO, Miguel. Seguridad en redes y seguridad de la información. [En línea]. Bogotá: Improvet. 2017., 80 p. Disponible en: <http://improvet.cvut.cz/project/download/C2ES/Seguridad_de_Red_e_Informacion.pdf>

Software Gurú, La Ética en el Hacking. [EN LÍNEA].2020. [Citado en 09 de octubre de 2021]. Disponible en internet: <https://sg.com.mx/revista/48/la-etica-el-hacking>

TECNOLOGUÍAS PARA EMPRESAS. “INGENIERÍA SOCIAL: EL HACKEO SILENCIOSO”. [En línea]. Marzo 2016. [13 octubre de 2021]. Disponible en: <http://www.enter.co/guias/tecnoguias-para-empresas/ingenieria-social-el-hackeosilencioso/.>

TEMPERINE, Marcelo. Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte. Buenos Aires, 2013, 12p. Trabajo de investigación (Doctorando en Derecho). Universidad Nacional del Litoral. Facultad de Ciencias Jurídicas y Sociales. Argentina.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Lección 6 Las Entidades territoriales [en línea]. [Consultado 09 de octubre de 2021]. Disponible en Internet en: <http://datateca.unad.edu.co/contenidos/109107/Contenido_en_linea/leccin_6_las_ entidades_territoriales.html>

.

# ANEXOS

**Anexo 1. Informe Controles**

INFORME DE LOS CONTROLES QUE PERMITAN MITIGAR EL RIESGO ASOCIADO A LAS VULNERABILIDADES IDENTIFICADAS

ELABORADO Y PROYECTADO POR

INGENIERO DE SISTEMAS

WALTER PORRAS

PIJAOS SALUD EPSI IBAGUE
ABRIL 2022

Tabla Contenido

Resumen Ejecutivo ..... 3
ABSTRACT ..... 4
INTRODUCCIÓN ..... 5
Objetivos ..... 6
1.1 Objetivo General ..... 6
Planteamiento del problema ..... 7
Resultado del estudio realizado ..... 8
1.2 Vulneravilidades encontradas en el sistema de información de la EPSI ..... 8
1.3 Alternativas de solución ..... 9
1.3.1 Actualización de Manual de Políticas de Seguridad ..... 9
1.3.2 Alternativa 2: Realizar una búsqueda de proveedor de seguridad Informática. ..... 10
1.4 Necesidad de Protección ..... 10

## Resumen Ejecutivo

Uno de los activos más valiosos para cualquier entidad es siempre su información almacenada. Dicha información Representa el conocimiento acumulado de años y la razón de ser del negocio. A pesar de ello, existen vulnerabilidades en los medios de almacenamiento digital de esta información, ante potenciales desastres tecnológicos que ponen en riesgo la integridad, el acceso y la administración de este activo.

Los encargados de resguardar este activo tan importante para la entidad reconocen esta situación y se enfocan en la búsqueda de una solución viable. Es por esta razón que se elabora este informe cuya finalidad es dar a conocer a la gerencia de la entidad la necesidad de implementar y actualizar la plataforma tecnológica de PIJAOS SALUD EPSI. Presentando una propuesta de valor que supla las necesidades de seguridad informática y correcta utilización de los recursos tecnológicos.

Para ello, y como resultado de este informe, se obtiene un perfil de la situación actual y la deseable según las necesidades actuales de PIJAOS SALUD EPSI y pensando en el crecimiento de la entidad, se identifican los requerimientos para disminuir la brecha tecnológica, los entregables permitirán satisfacer tales requerimientos y se elaborara un plan para la dirección del proyecto que busque implementarlos.

## ABSTRACT

One of the most valuable assets for any entity is always its stored information. This information represents the accumulated knowledge of years and the reason for being of the business. Despite this, there are vulnerabilities in the digital storage media of this information, in the face of potential technological disasters that put the integrity, access and management of this asset at risk.

Those in charge of safeguarding this important asset for the entity recognize this situation and focus on finding a viable solution. It is for this reason that this report is prepared, the purpose of which is to make the entity's management aware of the need to implement and update the technological platform of PIJAOS SALUD EPSI. Presenting a value proposition that meets the needs of computer security and correct use of technological resources.

For this, and as a result of this analysis, a profile of the current and desirable situation is obtained according to the current needs of PIJAOS SALUD EPSI and considering the growth of the entity, the requirements are identified to reduce the gap between the two, the Deliverables that will satisfy these requirements and a plan for project management seeking to implement them is prepared.

## INTRODUCCIÓN

PIJAO SALUD EPSI es una entidad que se encuentra en la actualidad operando a nivel nacional prestando sus servicios en 21 municipios en los departamentos de Risaralda, Tolima y Meta. Y que por el gran procesamiento de datos que se tiene requiere de una conectividad entre todas sus sedes y un manejo adecuado de la información procesada dando como prioridad a la seguridad de la misma. Es de suma importancia tener integrada esta información a nivel nacional en cada una de sus sedes con el fin mejorar la operatividad y unificar sus procesos dando la protección contra cualquier virus y/o amenazas que se pueda llegar a dar.

El equipo de sistemas y seguridad de la información de PIJAOS SALUD EPSI, ha identificado algunos problemas principalmente en la seguridad de sus conexiones a internet y en los accesos al servidor donde está alojada su información principal, En este informe también se plasma toda aquella información relevante para la solución de problemáticas similares y se documenta de manera adecuada toda aquella información que conlleve a un diagnóstico y una respuesta congruente con la problemática que se haya planteado.

## Objetivos

### 1.1 Objetivo General

Informar a la alta gerencia del estado real de la seguridad informática de PIJAOS SALUD EPSI con la finalidad de garantizar una mayor continuidad de negocio gracias a la disponibilidad de la red segura y tratamiento de seguridad de la información adecuada.

Objetivos específicos

Identificar los diferentes factores que afectan la continuidad del servicio debido a la falta de una protección adecuada.

Presentar un informe que relacione los controles que permitan mitigar el riesgo asociado a las vulnerabilidades identificadas para una correcta gestión de confidencialidad, integridad y disponibilidad de la información de la organización.

**Planteamiento del problema**

Pijaos Salud es una Entidad Promotora de Salud Indígena de carácter especial, que presta sus servicios al sector indígena del departamento del Tolima perteneciendo íntegramente al sector público especial de la salud en Colombia. Por esta razón y teniendo en cuenta que en la mayoría de los casos la seguridad de la información es el talón de Aquiles de las diferentes entidades públicas del sector salud en Colombia, debido a la pobre gestión que se realiza en cuanto a sus infraestructuras informáticas internas, sus redes, sus bases de datos y de más activos de información con los que cuentan. Esto hace que cada vez se vuelvan más vulnerables frente al gran crecimiento tecnológico que están teniendo los ciberdelincuentes en el país, poniendo en riesgo latente cada día su información y la continuidad del negocio que es la gestión de los recursos destinados por el gobierno para la salud de la población indígena del departamento del Tolima.

La falta de capacitación del personal encargado de la seguridad de la información y la inexistencia de un producto que pueda suplir la necesidad de seguridad protegiendo el activo más valioso de la entidad, se convierte en el problema más grande que se tiene debido a que el mundo informático esta día a día cambiando y generando nuevas amenazas que pueden llegar a ser tan perjudiciales para cualquier entidad. Dicha situación tiene en riesgo el correcto funcionamiento y productividad de la entidad, ya que se nos presentan diferentes factores que afectan la continuidad de la operación y que siguen interrumpiendo la toma de decisiones provocando pérdidas de información y tiempo, convirtiéndose en una gran pérdida de recursos económicos.

**Resultado del estudio realizado**

**METODOLOGÍA OS (OFFENSIVE SECURITY)** utilizada para realizar un hacking ético, mediante el análisis documental con el fin de conocer sus características, ventajas, desventajas y contextos de aplicación, dentro de la entidad. Con la finalidad de obtener los resultados para el respectivo análisis, se realizó una encuesta a los trabajadores de la entidad como fuente primaria de la información, permitiendo con está la obtención de datos relevantes y resolviendo las dudas e inquietudes que se tiene sobre el tema de estudio, con la finalidad de implementar diferentes alternativas de solución a los problemas encontrados.

Todo esto se realiza para determinar el estado actual de los sistemas de seguridad de la información de Pijaos Salud EPS Indígena sede Ibagué. En la actualidad se cuenta con diferentes metodologías y herramientas que son utilizadas en el trabajo de evaluar las diferentes vulnerabilidades que se puedan encontrar en un sistema de información, para este caso se emplearon diferentes herramientas de seguridad de la información y se utilizaron diferentes tipos de software que corren sobre el sistema operativo Linux, con el objetivo de hallar las vulnerabilidades en los sistemas de seguridad de la información implementados en la entidad.

Enfocando la búsqueda de alternativas en los resultados del análisis que se realizó mediante las diferentes pruebas y procesos de la metodología de hacking ético y pen test utilizadas y que nos mostraron diferentes vulnerabilidades de seguridad halladas en el sistema de información de Pijaos salud EPS Indígena Sede Ibagué, las cuales se presentaran a continuación:

### 1.2 Vulneravilidades encontradas en el sistema de información de la EPSI

- Identificación de versionamiento sin actualizar de algunos de los servicios que se encuentran corriendo actualmente sobre los puertos del servidor de la EPS INDIGENA se encuentran sin su debida actualización, haciendo que esto se convierta en una vulnerabilidad para la seguridad y una amenaza para el sistema de información de esta entidad.

- Se encuentran puertos abiertos y vulnerabilidades de la red que ponen en riesgo la seguridad de la información.

- No cuenta con los parches de seguridad para sistemas operativos Windows y genera una vulnerabilidad critica a la seguridad del sistema, permitiendo a un ciber atacante tomar control remoto del sistema operativo y generando pérdidas de control en el sistema, dando la oportunidad a un atacante de cargar algún código malicioso (malware) logrando contaminar toda una red por medio de los host que se encuentran vulnerables en esta red, Infectándolo y ejecutando el malware en la memoria del servidor sin necesidad de escribir absolutamente nada en el disco, siendo así indetectable para los ojos de los usuarios normales ya que no se crea ningún proceso nuevo.

- Robo, intrusión y perdida de archivos y demás bases de datos. PIJAOS SALUD se encuentra vulnerable ante este problema debido a que el control que se tiene no es lo suficientemente concreto debido a la falta de herramientas tecnológicas que permitan un correcto manejo de la información que sale de la EPSI.

- Falta de conocimiento de los estándares de seguridad de la información por parte de los funcionarios de la entidad, generando así una brecha de seguridad para la información que ellos

manejan, navegación imprudente y falta de capacitación de los empleados. Se presenta como riesgo en PIJAOS SALUD desde el mismo momento en que los funcionarios no respetan las políticas de seguridad de la información que se implementan dentro de la entidad y por el contrario ingresan a sitios prohibidos poniendo en riesgo los equipos de cómputo, las bases de datos y demás información que se trabaje en cada estación de trabajo, exponiendo el activo más valiosos de la entidad en páginas sin protección y con posibles atacantes Hackers que lo que buscan es ingresar a la entidad a robar información.

- Intrusión de Virus y Códigos maliciosos. En PIJAOS SALUD se tiene el potencial riesgo de infección de los equipos con virus y otros programas maliciosos que busquen infectar nuestros sistemas con el fin de copiar rastreadores que roban incluso claves de acceso, credenciales bancarias, tokens utilizados en la entidad para transacciones bancarias, entre otros datos fundamentales para las finanzas de PIJAOS sin dejar rastro en los dispositivos.

## 1.3 Alternativas de solución

### 1.3.1 Actualización de Manual de Políticas de Seguridad

Es necesario para la seguridad de la información de la Entidad el contar con una actualización de manual de políticas de seguridad de la entidad, con el fin de endurecer los controles de accesos y definir un plan de respuestas ante incidentes que permita dar tratamiento de una manera más adecuada a los diferentes peligros a los que se enfrenta la entidad en materia de seguridad en este momento.

No obstante es importante resaltar que la generación de esta actualización al manual de políticas de seguridad que se debe realizar tendrá que estar acompañada de personal experto en seguridad informática con la meta de cubrir todas las falencias que posee el actual manual y en busca de asegurar de la manera más adecuada la información que reposa en sus servidores. Dentro de estas se deben establecer unas políticas de seguridad de la información donde se pueda contemplar la realización de diferentes pruebas de penetración por medio de la metodología OS (OFFENSIVE SECURITY) teniendo en cuenta la importancia de detectar falencias y vulnerabilidades a tiempo.

Es de suma importancia el poder implementar dentro de las políticas de seguridad de la entidad un control de acceso de los usuarios más efectivo que pueda tener un verdadero impacto en la información que ingresa y también en la información que se extrae de las bases de datos de la entidad, teniendo como referente la falta de controles y la poca información que los empleados de la entidad, tomando como base los resultados del test de conocimiento realizado al personal. Se debe gestionar y actualizar sus políticas de creación de backups de las bases de datos, teniendo en cuenta que se encuentran una serie de falencias en los sistemas de seguridad de información de la entidad y puede llegar a presentarse perdidas de sus bases de datos eventualmente.

También es importante implementar dentro de la entidad una planeación más elaborada sobre los mantenimientos preventivos a los diferentes equipos de cómputo que tengan injerencia directa sobre el sistema de información de la EPS Indígena, esto referenciado por la metodología **OS (OFFENSIVE SECURITY)** establecida para el presente estudio con la finalidad de tener un control de vulnerabilidades realizando pruebas de manera regular a sus sistemas de información, realizando un proceso interno que sea el encargado de gestionar directamente la capacitación del personal involucrado en la seguridad de la información dentro de la entidad con el fin de actualizar conocimientos y evitar futuras intrusiones de terceros al sistema de información de la EPS Indígena. Ya que en las diferentes pruebas de penetración realizadas en el presente estudio se detectaron algunas falencias en sus sistemas de información.

### 1.3.2 Alternativa 2: Realizar una búsqueda de proveedor de seguridad Informática.

Por solicitud de la Gerencia de la EPSI se genera como alternativa 2 la posible adquisición de una plataforma de ciberseguridad más robusta, que permita que la organización enfoque sus recursos al desarrollo de su negocio. Prestando una correcta protección de los activos de información de la entidad, reduciendo costos operativos, en riesgos tecnológicos y salvaguarda de la información. Que se enfoque también en la gestión del conocimiento en la nueva plataforma involucrando al personal de la organización y difundiendo la información vital de una manera sistemática y eficiente con el fin de lograr un mejor desempeño en las áreas de la organización y mitigando el riesgo.

Se requiere un proveedor tecnológico que permita tener un rápido acceso a nuevas tecnologías previniendo una intrusión de terceros malintencionados que pongan en riesgo la continuidad del negocio, realizando una capacitación al personal encargado de salvaguardar la información y equipos tecnológicos de la entidad. Teniendo en cuenta que el equipo de sistemas y seguridad de la Información, es una de las áreas que a través de los años ha venido adquiriendo la experiencia necesaria de la mano de la administración y de los funcionarios a cargo para lograr la identificación de falencias, fallas, necesidades y vulnerabilidades que se presentan en el entorno tecnológico e informático de la entidad. Dicha experiencia ha logrado que el área de sistemas se convierta en un punto estratégico para la planeación e implementación de proyectos que busquen dar solución a los distintos escenarios desfavorables que se presenten frente a la prestación de servicios, perdida de datos o retrasos en el flujo de información entre los distintos actores del negocio.

### 1.4 Necesidad de Protección


Cordialmente,

WALTER KELIN PORRAS
Ingeniero de Sistemas