ANÁLISIS DE SEGURIDAD A UNA ARQUITECTURA WEB UTILIZADA PARA LA ENTREGA DE RESULTADOS DE LABORATORIOS CLÍNICOS.

PRESENTADO POR:
FABIÁN DAVID GONZÁLEZ ROMERO
GERARDO PIÑEROS PUENTES
SEBASTIÁN TIBADUIZA CALDERÓN

ASESOR TÉCNICO DE PROYECTO:
WILSON MAURO ROJAS REALES

UNIVERSIDAD EL BOSQUE
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD EN REDES TELEMÁTICAS
BOGOTÁ, COLOMBIA
enero de 2021

CONFIDENCIAL

Este documento se ha realizado únicamente con fines educativos, por lo que la persona que está interactuando con esta información, actúa bajo su propia responsabilidad y debe tener en cuenta la reglamentación de la seguridad de la información de la república de Colombia bajo la ley 1273 del 2009.

Dedicatoria

El viento sopla a su debido momento,
Con la ayuda de su árbol madre,
Se eleva cada hoja del suelo,
Logrando lo inimaginable.

A nuestras familias.

Agradecimientos

El presente equipo de trabajo quisiera manifestar el más profundo agradecimiento en estas líneas por la ayuda que muchas personas, docentes y colegas nos prestaron durante lo que fue este proceso de realización y redacción de este trabajo.

Como pilar fundamental a nuestros círculos familiares los cuales han ayudado y apoyado en todo nuestro esfuerzo, a nuestro director, Wilson Rojas, por orientarnos en todos los momentos que fueron necesarios sus consejos.

Así mismo, expresamos los más sinceros reconocimientos a la Universidad el Bosque por todas las atenciones e información brindada a lo largo de este proceso de formación.

Contenido

Lista de ilustraciones

Lista de tablas

RESUMEN

En la actualidad, los sistemas de información han tomado parte fundamental de la sistematización de procesos, con la presencia de eventos no convencionales como la presencia del Covid-19, estos sistemas y arquitecturas en las diferentes organizaciones del sector salud que manejan procesos de entrega de resultados clínicos, la necesidad por garantizar a los pacientes la veracidad de la información transmitida desde los centros clínicos se ve en aumento significativo.

La gestión de este proceso requiere, como todo sistema de información, la definición de normas o parámetros de uso y administración adecuada. El presente trabajo se direcciona a ejecutar un análisis de riesgos de la arquitectura web del proceso de entrega de resultados clínicos de una organización, en el que por medio de diferentes técnicas de análisis de vulnerabilidades de seguridad de la información, pretende identificar los riesgos con mayor criticidad de impacto y probabilidad, para realizar una propuesta de mejora recomendando controles o medidas de protección correspondientes al riesgo para proteger la disponibilidad, integridad y confidencialidad de la información de la organización.

PALABRAS CLAVE

Análisis de vulnerabilidades, Integridad, Confidencialidad, Disponibilidad, Arquitectura web, Riesgos.

ABSTRACT

Nowadays, information systems have taken a fundamental part in the process' systematization, due to the unconventional events' presence such as the Covid-19, these systems and architectures in the different health sector organizations, are managing processes of delivery clinical results with the need to guarantee the veracity to the patients from them information transmitted from clinical centers is increasing significantly.

The management of this process requires, like any information system, the standard or parameters' definition for use and proper administration. This work is aimed at executing a risk analysis of a web architecture to the delivering clinical results' process for an organization, in which, through different techniques of information security vulnerabilities' analysis, it aims to identify the risks with the most criticality among impact and probability values, to make a proposal improvement, recommending controls or protection measures for each detected risk to protect the organization's information's availability, integrity and confidentiality.

KEYWORDS

Vulnerability analysis, Integrity, Confidentiality, Availability, Web architecture, Risks.

1. TÍTULO

ANÁLISIS DE SEGURIDAD A UNA ARQUITECTURA WEB UTILIZADA PARA LA ENTREGA DE RESULTADOS DE LABORATORIOS CLÍNICOS.

2. INTRODUCCIÓN

Con los avances tecnológicos y las necesidades urgentes de una comunicación efectiva y veraz en todos los sectores, incluyendo el sector salud, pilar importante y vital, al ser este un derecho fundamental de la sociedad.

Estos avances tecnológicos, conllevan grandes desafíos a nivel de la seguridad de la información, toda vez que la ciberdelincuencia es un problema que, día tras día mejoran tanto sus técnicas como sus tácticas mediante el engaño o ataques cada vez más sofisticados a la infraestructura informática, esto con la finalidad de vulnerar la seguridad de los usuarios y así recopilar información sensible, y de acceso restringido, para realizar estafas o afectar servicios importantes de la organización.

Según un informe realizado por la Cámara Colombiana de Informática y Telecomunicaciones (CCIT), ha aumentado 37% la ciberdelincuencia en Colombia relacionada con el COVID-19. La ciberseguridad ha tomado uno de los papeles más importantes a nivel mundial, de esto depende la protección de la información tanto de empresas como de personas. En el primer trimestre de 2020, se presentaron 7.082 denuncias por ciberdelitos lo que representa un incremento del 27%, comparado con en el mismo periodo de 2019.[1]

Ante esta situación, hemos querido, a través de nuestro trabajo incrementar herramientas que permitan que esta información, entre médicos y pacientes, que transitan en la internet, abarcando datos sensibles y que son fuente de información para la determinación de procedimientos médicos; no sea vulnerada al estar expuesta en la web y a disposición de cualquier individuo malintencionado; por tal motivo, se hace urgente y necesario, proteger y asegurar su integridad y confidencialidad, tal como fue emitido desde su fase inicial.

Teniendo en cuenta lo anterior, se ha desarrollado este proyecto para aplicar los conceptos aprendidos durante la especialización en Seguridad en Redes Telemáticas mediante el análisis, evaluación de vulnerabilidades y análisis de riesgos de las amenazas detectadas y así garantizar la Seguridad de la Información sobre los resultados emitida por un laboratorio clínico.

Con este proyecto se pretende contribuir en la seguridad de la información para el paciente en cuanto a la entrega de resultados de laboratorios clínicos y así proteger la integridad y confidencialidad de los exámenes de su transmisión de origen a destino.

3. DESCRIPCIÓN GENERAL DEL PROYECTO

3.1 DEFINICIÓN DEL PROBLEMA

Debido a la transformación tecnológica y digital que ha impactado los diferentes sectores de la salud, se ha hecho indispensable y de mayor facilidad la publicación de resultados de laboratorio clínico directamente por medio de la web. Para que los usuarios puedan visualizar y descargar estos resultados, es necesario que el usuario acceda a la plataforma mediante un usuario y una contraseña.

Actualmente la entidad de salud no posee mecanismos de seguridad que le permitan controlar el flujo de información, esto es algo de sumo cuidado precisamente porque se está trabajando con datos sensibles.

La aplicación web que hoy día posee la entidad está alojada en un servidor que no garantiza la confidencialidad e integridad de la información. El servidor donde se encuentra alojada la aplicación no cuenta con certificado digital, para proteger el transporte de la información. Tampoco cuenta con protección a la integridad de la información emitida en el PDF por medio de algún mecanismo que permita asegurar la integridad de la información registrada. Al no tener asociado un DNS a la página donde se realiza la publicación del sitio es totalmente vulnerable a un ataque teniendo de primera mano la información de la dirección lógica (IP) pública y el puerto por el cual se entrega la información.

Por otro lado, la arquitectura que hoy día posee la solución no ofrece mecanismos de seguridad. Se trata de una arquitectura de dos capas lo cual presenta entre algunas de las desventajas: la instalación de todos los componentes de software en una sola máquina. En este caso, se tiene un nivel de riesgo alto ante cualquier ataque informático sobre la máquina. La ineficiencia en el uso del hardware utilizado, el diseño propuesto inicialmente no es modular, dificulta la partición de un problema complejo con la implementación y/o detección del mismo, limitación para establecer niveles de seguridad frente a los objetos propios establecidos.

Con lo anterior se puede incurrir en posibles ataques a vulnerabilidades expuestas y su tiempo de respuesta se extienda en el tiempo ya que no se encuentre de manera efectiva. Como ejemplo

se encuentra: Vulnerabilidad por inyección de código, indexación de directorios, detención de tráfico de información (usuarios y contraseñas), phishing, desbordamiento de búfer, entre otros. A continuación, se presenta el diagrama de arquitectura actual:

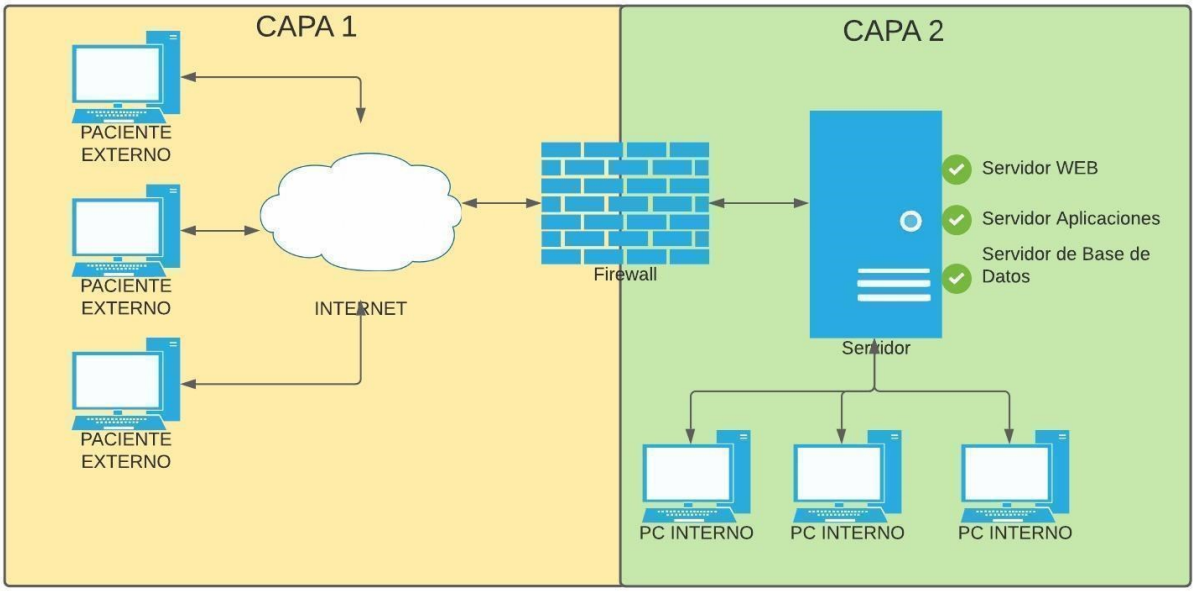

Ilustración 1 Diagrama de Componentes estado actual

3.2 ASPECTOS A SOLUCIONAR

Uno de los mayores aspectos a solucionar es el diseño de una nueva arquitectura. Y esta arquitectura mínima debe ser de tres capas de tal manera que se logre independizar el componente de bases de datos y la aplicación.

Otro aspecto importante para solucionar es el transporte de los datos, esto se consigue instalando un certificado digital a la página en donde actualmente los usuarios finales realizan sus descargas, también teniendo en cuenta la implementación de un nombre de dominio al sitio y obtener un nombre del sitio más seguro.

Otro de los aspectos importantes que debe ser solucionado atenta contra la integridad de la información específicamente en el tratamiento de los datos que son registrados en un documento PDF. También se debe solucionar la confidencialidad que se está aplicando al mismo, esto por medio de la generación automática de una contraseña desde la descarga que realiza el usuario final.

3.3 SOLUCIÓN PROPUESTA

Se propone realizar una propuesta de mejora a partir de un análisis de vulnerabilidades y riesgos de la arquitectura web actual para el proceso de entrega de resultados clínicos, para una empresa prestadora de servicios de salud, teniendo como objeto a evaluar la seguridad de la información en cuanto a la arquitectura web y el proceso de entrega de resultados al paciente. Basado en dicho análisis, presentar un esquema de novedades de seguridad en las que expongan los componentes de la arquitectura web, este análisis facilitará la identificación de puntos débiles, los cuales se enfocarán para generar controles de los diferentes aspectos de la seguridad de la información. Además de esto, proponiendo y documentando como especialistas en Seguridad de redes telemáticas, pautas de seguridad de la información y recomendaciones para asegurar los tres pilares (disponibilidad, integridad, confidencialidad) en aras de que sean evaluados por la organización para una futura toma de decisiones.

4. ESTADO DEL ARTE

4.1 MARCO DE REFERENCIA TEÓRICO

En Colombia la entidad de salud COOMEVA EPS, ubicada en la ciudad de Cali, la sede principal, pero que actualmente ofrece los servicios a nivel nacional, con sus diferentes sedes regionales. Actualmente ofrece a sus pacientes la posibilidad de descargar sus resultados clínicos, por medio de la IPS CHRISTUS SINERGIA. La IPS hace entrega de resultados clínicos por medio del portal Web. Este portal utiliza el protocolo https, el cual brinda una capa de seguridad, ya que cuenta con certificados digitales. Adicionalmente, el portal web exige a sus pacientes o usuarios, registrarse para poder adquirir los resultados clínicos. Luego de este registro el usuario, debe iniciar sesión en el portal con un correo electrónico, contraseña y elegir el rol de paciente ya que también se encuentra el rol de Médico especialista. Una vez dentro, se selecciona la pestaña de laboratorio clínico, para entrega de resultados y debe ingresar el número de identificación de la cédula de ciudadanía y darle click al consultar. Al darle click a botón consultar, muestra los exámenes clínicos del paciente y al darle click se descarga un archivo PDF con los resultados clínicos.

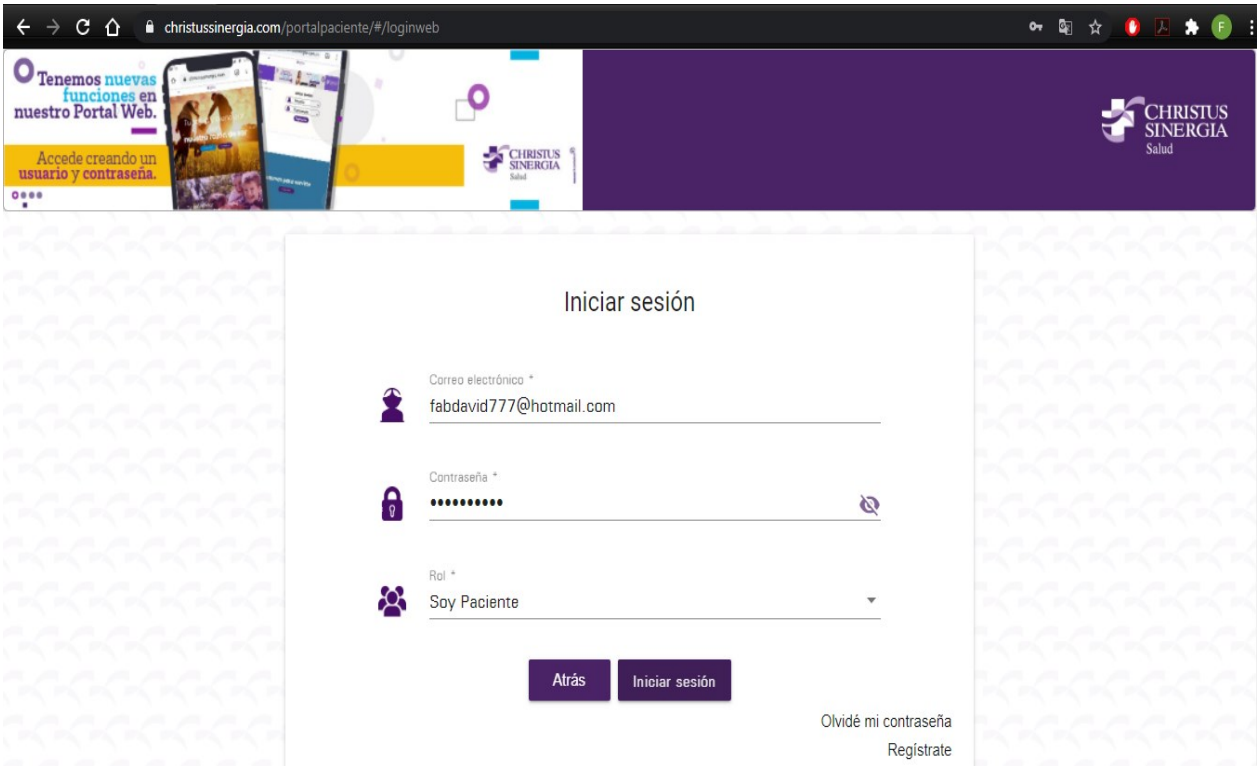

Ilustración 2 Página web Chistus Sinergia

En la ciudad de Pereira, la empresa ANALIZAR LABORATORIO CLÍNICO, traslada la oficina principal a la ciudad de Bogotá, y a partir de allí, comienza una importante expansión geográfica en toda Cundinamarca.

Estos, ofrecen a sus usuarios (pacientes) la probabilidad de descargar sus resultados clínicos. La empresa ANALIZAR LABORATORIO CLÍNICO, realiza la entrega de resultados por medio del portal Web. Este portal utiliza el protocolo https, el cual brinda seguridad, ya que cuenta con certificados digitales esenciales para dar confianza al paciente. El portal web, pide al usuario, credenciales de acceso que son suministrados por el laboratorio, por medio de un correo electrónico. Ya teniendo la credencial de acceso, éstas, son puestas en los campos correspondientes. Una vez realizado este proceso, dan click en el botón ingresar. Luego de visualizarlos, pueden darle click al examen que quieren obtener y descargar en un archivo PDF.

Ilustración 3 Página web Analizar Laboratorio Clínico

La organización Higuera Escalante, encargada de la prestación de servicios de salud integrales, seguros, oportunos y de alta confiabilidad en las áreas de laboratorio clínico, entre otras especialidades, extraído directamente de su definición como negocio, esta organización tiene un proceso de entrega de resultados clínicos para pacientes y entidades como una de las líneas de servicio principales de su actividad de negocio, por medio de la página web, pensando en la comodidad de los pacientes, es habilitado un botón de “Descarga de resultados”, el cual una vez se da click en esta opción, automáticamente se abre una nueva pestaña con datos a diligenciar, tales como la Orden de servicio, Identificación (sin puntos o comas) y un captcha como factor de seguridad para la comprobación de que no es un robot. Finalmente, una vez se realice el proceso se descargará el resultado acorde a la información suministrada en formato PDF. Tal como se puede ver en la siguiente imagen, para este caso la página web no es https y no se requiere de una autenticación previa para el acceso al descargue de resultados.

Ilustración 4 Página web Higuera Escalante

Compensar EPS es una organización de servicios y planes de bienestar, con un portafolio de servicios que permite la centralización de condiciones laborales entre empresa y afiliados, realizando una integración de servicios en diferentes canales de comunicación. En este caso nos enfocamos en los procesos de descarga de certificados directamente en la plataforma web, donde se evidencia la existencia de un certificado digital, seguido de una autenticación del usuario y por medio de una serie de pasos la ejecución de descarga del certificado el cual pide como factor de seguridad la digitación de un password o contraseña, para la visualización e interacción con el certificado a descargar, de lo contrario no será posible realizar ninguna acción bajo este certificado generado.

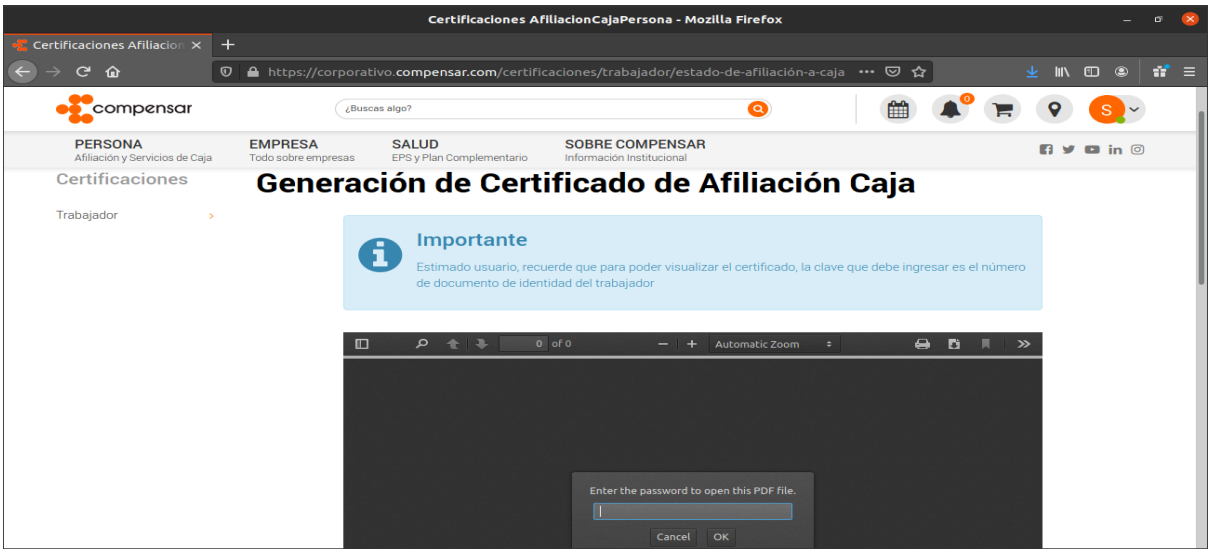

Ilustración 5 Página web Compensar

4.2 MARCO DE REFERENCIA TECNOLÓGICO

Teniendo en cuenta lo anteriormente mencionado en el marco teórico, las entidades COOMEVA EPS y ANALIZAR LABORATORIO CLÍNICO, una vez consultadas, no hacen uso de controles de seguridad para la entrega de resultados de laboratorios clínicos, al no aplicar seguridad al archivo PDF.

El caso de HIGUERA ESCALANTE el hecho de no tener un cifrado de datos por medio de un certificado digital, será vulnerable a posibles sniffers los cuales podrán visualizar el tráfico transmitido hacia y por la red, interceptando información sensible, adicionalmente se debe revisar el flujo entre las páginas web ya que no se requiere un filtro de autenticación para el acceso a esta página.

Para el caso de COMPENSAR, se puede evidenciar un sistema más completo que los anteriores, con certificados digitales, proceso de autenticación, flujo correcto de páginas web y seguridad bajo verificación en la descarga de archivos.

Uno de los controles para reforzar y garantizar la triada de la información. Se basa en ir al código fuente donde se genera los PDF y mediante la librería que se utiliza para el armado de los mismos adicionar la seguridad la apertura con clave y a su vez generar el control de seguridad del proceso, al mismo tiempo agregar la librería que genere una firma digital al documento PDF que se está creando. Este proceso se realiza de manera interna en el servidor al momento de generar una petición de creación de un PDF con los datos ingresados del paciente en cuestión, con el fin de garantizar el manejo de la información y la integración de los mismos al interior de la organización.

5. GLOSARIO DE TÉRMINOS

Confidencialidad: Confidencialidad es la cualidad de confidencial (que se dice o hace en confianza y con seguridad recíproca entre dos o más individuos). Se trata de una propiedad de la información que pretende garantizar el acceso sólo a las personas autorizadas. [2]

Integridad: El concepto de integridad, que deriva del término de origen latino integristas, hace hincapié en la particularidad de íntegro y a la condición pura de las vírgenes. Algo íntegro es una cosa que posee todas sus partes intactas o, dicho de una persona, hace referencia a un individuo

correcto, educado, atento, probo e intachable. [3]

Laboratorio Clínico: El laboratorio clínico es el lugar donde un equipo multidisciplinario formado por el químico clínico, analista clínico o médico patólogo clínico, los profesionales del laboratorio y los técnicos en análisis clínicos, analizan muestras biológicas humanas que contribuyen al estudio, prevención, y hacen investigación viable para el cuerpo humano. [4]

Historia Clínica: Conjunto de documentos en el que se contienen los datos, valoraciones e informaciones de cualquier tipo sobre la situación y evolución clínica de un paciente a lo largo de su proceso asistencial. [5]

Web: Web es un vocablo inglés que significa “red”, “telaraña” o “malla”. El concepto se utiliza en el ámbito tecnológico para nombrar a una red informática y, en general, a Internet (en este caso, suele escribirse como Web, con la W mayúscula). [6]

Sistema Operativo CentOS: CentOS (Community ENTerprise Operating System) es una bifurcación a nivel binario de la distribución GNU/Linux Red Hat Enterprise Linux RHEL, compilado por voluntarios a partir del código fuente publicado por Red Hat. Es un sistema operativo de código abierto, basado en la distribución Red Hat Enterprise Linux, operándose de manera similar, y cuyo objetivo es ofrecer al usuario un software de "clase empresarial" gratuito. Se define como robusto, estable y fácil de instalar y utilizar. Desde la versión 5, cada lanzamiento recibe soporte durante diez años, por lo que la actual versión 7 recibirá actualizaciones de seguridad hasta el 30 de junio de 2024. [7]

Apache Tomcat: Apache Tomcat (también llamado Jakarta Tomcat o simplemente Tomcat) funciona como un contenedor de servlets desarrollado bajo el proyecto Jakarta en la Apache Software Foundation. Tomcat implementa las especificaciones de los servlets y de JavaServer Pages (JSP) de Oracle Corporation (aunque creado por Sun Microsystems). [8]

Máquina Virtual: Una máquina virtual de sistema es aquella que emula a un ordenador completo. En palabras llanas, es un software que puede hacerse pasar por otro dispositivo -como un PC- de tal modo que puedes ejecutar otro sistema operativo en su interior. Tiene su propio disco duro, memoria, tarjeta gráfica y demás componentes de hardware, aunque todos ellos son virtuales. [9]

Memoria RAM: Es la memoria principal de un dispositivo, esa donde se almacenan de forma temporal los datos de los programas que estás utilizando en este momento. Sus siglas significan Random Access Memory, lo que traducido al español sería Memoria de Acceso Aleatorio, y es un tipo de memoria que te puedes encontrar en cualquier dispositivo, desde ordenadores de sobremesa hasta teléfonos móviles. [10]

Procesador Core: Intel Core es la principal línea de microprocesadores de Intel para el mercado de ordenadores de consumo. Se ofrecen en versiones Intel Core i7, i5 e i3, además de otras como Core M de ultra bajo voltaje y otras marcas como Pentium o Celeron. [11]

PDF: PDF (sigla del inglés Portable Document Format, «formato de documento portátil») es un formato de almacenamiento para documentos digitales independiente de plataformas de software o hardware. Este formato es de tipo compuesto (imagen vectorial, mapa de bits y texto). [12]

Paciente: Persona que necesita cuidados para el mantenimiento o recuperación de la salud, y para lo que requiere asistencia sanitaria. [13]

6. JUSTIFICACIÓN

Siendo la salud un derecho fundamental, es importante, que, al interior de las empresas prestadoras del servicio, se garantice, agilidad y un mayor control sobre la información que se emite y que se guardan en cada uno de los servidores del cliente, para perseverar por la seguridad de la información del paciente.

Un ejemplo claro, lo tenemos hoy en día, toda vez que el uso de la información del sector salud se está transmitiendo, en su mayoría por internet, presentando una brecha de seguridad considerable en cuanto a vulnerabilidades de la información, expuesta a diversas técnicas de suplantación y pérdida de información por los medios publicados en la web.

Dicho esto, surge la necesidad de proteger la información que emite la comunidad médica, para evitar que presuntos ciberdelincuentes ejecuten acciones maliciosas que afecten y vulneren los datos de clientes y/o pacientes, lo que ocasionaría actos falseados y resultados adversos al fin propuesto del proceso en este caso de la entrega de resultados clínicos.

Por lo antes mencionado, el presente trabajo, propone a las empresas prestadoras del servicio de salud, generar controles de seguridad que permitan realizar validaciones de la autenticidad de

un documento descargado desde el aplicativo web de la organización de salud; por medio de contraseñas personalizadas, para cada uno de sus usuarios, pacientes. Además, enfatizar sobre políticas de seguridad y en la sensibilidad de la información.

Cabe anotar que según cifras de la Cámara Colombiana de Informática y Telecomunicaciones (CCT), la violación de datos personales está ubicado en el segundo lugar en Colombia con 8.037 casos. Este dato revela que la segunda amenaza en Colombia para empresas y ciudadanos es el robo de identidad.

7. OBJETIVOS

7.1. GENERAL.

Documentar el análisis de seguridad para arquitectura web del proceso de entrega de resultados de laboratorios clínicos, instalada actualmente en los clientes de la organización, generando una propuesta de mejora a través de la identificación de riesgos y vulnerabilidades donde se evalúa la integridad y confidencialidad de la información.

7.2. ESPECÍFICOS

- Identificar los componentes relacionados al diseño actual de la arquitectura web del proceso de entrega de resultados clínicos.
- Analizar y evaluar los componentes relacionados al diseño actual de la arquitectura web del proceso de entrega de resultados clínicos.
- Elaborar matriz de identificación y evaluación de riesgos de seguridad informática, para el proceso de entrega de resultados clínicos.
- Elaborar propuesta de mejora de seguridad, para minimizar los riesgos existentes en la integridad y confidencialidad de la información en el proceso de entrega de resultados clínicos.

8. REQUERIMIENTOS

- Documento estado actual de integridad y confidencialidad de la información en la entrega de resultados clínicos.
- Matriz de riesgos para analizar las vulnerabilidades del proceso de entrega de resultados clínicos a pacientes y/o clientes de la organización.
- Documento propuesto de mejora de seguridad para la integridad y confidencialidad en la entrega de resultados clínicos.

- Formato de requerimientos necesarios para ampliar la confidencialidad e integralidad de la información emitida en los PDF por la arquitectura actual.

9. METODOLOGÍA

La metodología implementada para el desarrollo del proyecto se ha determinado respecto a las fases de desarrollo de cada uno de los puntos claves que serán indispensables para que el flujo de trabajo sea ágil y preciso en cada una de las acciones, para una eficiente ejecución de acciones con la mejor media de optimización de los procesos.

A continuación, se describe cada una de las fases propuestas para el flujo de trabajo del proyecto:

9.1 FASE 1: ANÁLISIS (LEVANTAMIENTO DE INFORMACIÓN)

Análisis, se define como el conocimiento inicial del proyecto, esta fase cuenta con las acciones iniciales de validación del entorno de trabajo y filosofía de operación de la herramienta, el cómo funciona, para quién funciona y cuál es el modo de operación de la misma, esto con la finalidad de obtener la mayor cantidad de información posible para el posterior tratamiento de la misma, centrando y direccionando lo recopilado orientado a las siguientes fases y objetivos.

9.2 FASE 2: IDENTIFICACIÓN (RIESGOS)

Identificación, cumple con el acotamiento de la información proporcionada por la fase de Análisis, sesgando y cerrando brechas de información que no se encuentra en el alcance del proyecto, esto para la identificación de los riesgos y/o vulnerabilidades de cada uno de los aspectos encontrados a nivel de la herramienta y arquitectura a analizar, generando una matriz de evaluación de lo antes mencionado, con la finalidad de cuantificar y dar por conocido cada uno de los aspectos a mejorar para emplear un plus de seguridad en la arquitectura evaluada.

9.3 FASE 3: DESARROLLO (PROPUESTA)

Desarrollo, define lo que sería el paso a seguir de la fase de la identificación de riesgos y vulnerabilidades, para documentar acciones de mejora a cada uno de los ítems presentados anteriormente, consolidando la información analizada e identificada, con la finalidad de realizar una propuesta de mejora del proceso en términos de seguridad de la información, concisa y aplicable al alcance del proyecto.

9.4 FASE 4: EJECUCIÓN (REQUERIMIENTO TÉCNICO)

Ejecución, cuenta como la última fase del proyecto, como última parte de la cadena de procesos, se proyecta a la entrega final por medio de un requerimiento formal y técnico hacia el área de TI

de la organización, consolidando el proceso de análisis, identificación y desarrollo de lo que serían las brechas de seguridad potencialmente vulnerables en la arquitectura web al momento de realizar la entrega de resultados clínicos a pacientes y/o clientes, con la finalidad de mejorar en términos de seguridad de la información, la entrega de forma digital y segura a dichas personas, en un entorno digitalizado por necesidad de las diversas situaciones a nivel global.

10. ESTADO ACTUAL

10.1 ANÁLISIS DEL ESTADO ACTUAL DE LA ARQUITECTURA WEB

10.1.1 PUERTOS

10.1.1.1 HERRAMIENTA DE ANÁLISIS DE PUERTOS

Para la identificación del estado actual de la arquitectura web para el proceso de entrega de resultados clínicos, se plantea realizar inicialmente el reconocimiento del entorno de la página web donde se permite él envió de resultados clínicos, la acción descrita se ejecuta por medio de la herramienta de código abierto NMAP, la cual tiene como función principal el rastreo y escaneo de puertos, esto con la finalidad de identificar la seguridad en el servidor, por medio de los puertos que se utilizan vs los puertos que están abiertos y pueden considerarse como potencial amenaza de un ataque cibernético.

10.1.1.2 ANÁLISIS DE PUERTOS

Debido a lo anterior se procede a ejecutar el análisis con el siguiente resultado:

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-18 05:32 Hora est. Pacífico, Sudamérica
Nmap scan report for [redacted].190.static.ifxnetworks.com (190.[redacted])
Host is up (0.0073s latency).
Not shown: 993 filtered ports
PORT     STATE  SERVICE
25/tcp   open   smtp
80/tcp   open   http
113/tcp  closed ident
5432/tcp open   postgresql
8080/tcp open   http-proxy
9090/tcp closed zeus-admin
9595/tcp open   pds
Aggressive OS guesses: Linux 2.6.32 (91%), Linux 2.6.32 - 3.1 (91%), Linux 3.10 (91%), Linux 3.2 (91%),
2.6.39 (89%), Linux 3.10 - 4.11 (89%), Apple macOS 10.13 (High Sierra) (Darwin 17.0.0) (88%), Linux 3.4
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.76 seconds
```

Ilustración 6 Escaneo NMAP entorno Windows

10.1.1.3 RESULTADOS DEL ANÁLISIS DE PUERTOS

Se identifican 5 (cinco) puertos abiertos, vulnerables y de fácil acceso para el ciber atacante. (25TCP, 80/TCP, 5432/TCP, 8080/TCP, 9595/TCP).

Al tener estos puertos expuestos en la web, es posible generar un exploit, es decir, una explotación de una vulnerabilidad o puerta trasera, de cada uno de los puertos, afectando la

funcionalidad normal de la operación en la arquitectura actual.

A continuación, se presenta en detalle, los servicios y descripción de cada uno de los puertos asociados al resultado expuesto por el resultado del análisis con la herramienta NMAP:

# Puerto	Estado	Protocolo	Servicio	Descripción
25	Open	tcp (Protocolo de Control de Transmisión)	smtp	SMTP Simple Mail Transfer Protocol (Protocolo Simple de Transferencia de Correo).
80	Open	tcp (Protocolo de Control de Transmisión)	http	HTTP HyperText Transfer Protocol (Protocolo de Transferencia de HiperTexto) (WWW).
113	Closed	tcp (Protocolo de Control de Transmisión)	auth	ident (auth) antiguo sistema de identificación.
5432	Open	tcp (Protocolo de Control de Transmisión)	postgresql	PostgreSQL, también llamado Postgres, es un sistema de gestión de bases de datos relacional orientado a objetos y de código abierto, publicado bajo la licencia PostgreSQL.
8080	Open	tcp (Protocolo de Control de Transmisión)	http	HTTP HTTP-ALT ver puerto 80. Tomcat lo usa como puerto por defecto.
9090	Closed	tcp (Protocolo de Control de Transmisión)	zeus-admin	Zeus Web Server es un servidor web propietario descontinuado para Unix y plataformas similares a Unix (incluyendo Solaris, FreeBSD, HP-UX y Linux).
9595	Open	tcp (Protocolo de Control de Transmisión)	pds	Servicio de detección de ping.

Tabla 1 Análisis de puertos

Procedemos con la profundización de los puertos presentados en estado Open o abierto, los cuales serían causales de posibles brechas de seguridad para la arquitectura web actual.

El puerto TCP 25, que provee el protocolo SMTP, al estar en estado abierto, presenta las siguientes vulnerabilidades:

- **Ataques DDoS tipo Port Flood por SMTP:** Este tipo de ataques de denegación de servicio, son bastante comunes en la actualidad, con lo que pretenden saturar en peticiones el puerto para el envió de correos SMTP, aumentando el tráfico, aprovechamiento de recursos y la posterior indisponibilidad del servicio y servidor, vulnerando la disponibilidad de la información.
- **SMTP CVE 2010-4344:** Exim es un servicio de mensajería utilizado por sistemas en base Unix, tal como el sistema operativo Linux, esto afectaría directamente al sistema operativo de la misma distribución de la arquitectura actual. Una vulneración del protocolo SMTP de acceso sea vulnerado, el ciberdelincuente tendría un escalamiento de permisos (vulnerabilidades reportadas como CVE 2010-4344 y CVE 2010-4345). Exim se presenta como vulnerabilidad de desbordamiento que permite a ciberdelincuentes, de manera remota ejecutar código con privilegios de dominio, con el objetivo de realizar escalamiento de los mismos y tomar control del servidor de la arquitectura.
- **SMTP CVE 2011-1720:** Cyrus SASL es la victima de esta vulnerabilidad que busca vulnerabilidades de autenticación del protocolo SMTP, lo cual, en caso de ser exitoso, se podrían ejecutar ataques de denegación de servicio, obteniendo la indisponibilidad del servicio de manera remota.

El puerto TCP 80, que provee el protocolo HTTP, al estar en estado abierto, presenta las siguientes vulnerabilidades:

- **Flooding:** Ataque de desbordamiento de buffer que presentara una potencial denegación de servicios por el exceso de paquetes y peticiones enviadas por el presunto atacante.
- **Netcat:** Herramienta de red que permite interpretar comandos para la apertura de puertos en un host, actuando como sniffer, que asocia un shell a un puerto concreto y forzar conexiones UDP/TCP.
- **HTTP CVE 2009-1890:** De criticidad alta en el demonio httpd Apache server para versiones 2.2.21, el cual permite realizar ataques de denegación de servicio por consumo

excesivo de recursos de CPU, perjudicando la disponibilidad del servidor, afectando la funcionalidad de la arquitectura web.

- **HTTP CVE 2017-7679:** De criticidad alta en el demonio httpd Apache server para versiones 2.2.21, permitiendo el acceso, obviando el proceso de autenticación y ocasionar ataques de denegación de servicios y/o escalamiento de privilegios en el servidor, afectando no solo la disponibilidad, sino también la integridad y confidencialidad de la información de las bases de datos.
- **HTTP CVSS 10.0:** De criticidad alta en el demonio httpd Apache server para versiones 2.2.21, donde no se presenta ningún tipo de soporte para la versión debido a su fin de producción. En esta vulnerabilidad, la actualización es fundamental para evitar este tipo de vulnerabilidades.

El puerto TCP 5432, que provee el protocolo HTTP, al estar en estado abierto, presenta las siguientes vulnerabilidades:

- **Brute force:** El uso del módulo auxiliar scanner/postgres/postgres_login, de metasploit, permite la ejecución de ataques de fuerza bruta utilizando ataques de diccionario para autenticarse en el servidor y obtener escalamiento de privilegios, afectando la integridad, confidencialidad y posible afectación de la disponibilidad del servidor y arquitectura web.
- **CVE 2015-3165:** Ataque remoto para el bloqueo o denegación del servicio por medio del cierre de sesiones SSL, en el tiempo de espera de la autenticación, presentando indisponibilidad en los servicios.
- **CVE 2015-4644:** Vulnerabilidad perteneciente a la función php_pgsql_meta_data, la cual no realiza la validación de la extracción del token de nombre de las tablas, permitiendo la denegación del servicio por eliminación de punteros Null.
- **CVE 2015-5288:** Derivado de la función crypt en pgcrypto, permitiendo a los ciber atacantes la potencial causal de una ejecución de denegación de servicio en recursos de memoria del servidor. Provocando el desbordamiento de búfer.
- **CVE 2016-5423:** Permite a usuarios remotos autenticados, la obtención de información confidencial por medio de ejecución de código de manera arbitraria por medio de escalamiento de privilegios, así mismo permite la denegación de servicio.
- **CVE 2015-5424:** PostgreSQL para este reporte permitía usuarios remotos autenticados, con rol de CREATEDB o CREATEROLE, escalar permisos para super-usuario.
- **CVE 2015-7048:** Instalador de PostgreSQL permite a los atacantes de manera remota

ejecutar código sin novedad a través del uso de puertos HTTP, mientras se realiza el proceso de descarga del software.

El puerto TCP 8080, que provee el protocolo HTTP, al estar en estado abierto, presenta las siguientes vulnerabilidades:

- **Ataque CGI:** Se denomina como el método de transmisión de información hacia un compilador ubicado en el servidor, el cual su función principal recae en la interacción de documentos web por medio de HTML, presentando la explotación de forma masiva a diferentes direcciones IP inyectando código para la generación de peticiones GET en el servidor.
- **Buffer Overflow:** Se denomina como el exceso de cantidad de memoria asignado por el sistema operativo, el cual satura los recursos de la máquina, presentando indisponibilidad en los servicios, a lo que se recomienda generar controles y alertas tempranas por medio de aplicaciones de monitoreo de recursos, para poder mitigar brechas de seguridad que puedan perjudicar el impacto de la aplicación frente al usuario final.
- **Denegación de servicio:** Derivado del buffer overflow, tiene como objetivo la indisponibilidad total de un sistema o arquitectura, en este caso, una potencial indisponibilidad en la arquitectura actual, presentaría el impacto critico en no poder realizar la entrega de resultados clínicos a los pacientes, lo cual termina siendo una incidencia de carácter critica o mayor, por lo tanto se requerirá de personal y grupos resolutores apropiados para la respectiva restauración de los servicios, su arquitectura y sistema.

El puerto TCP 9595, puerto del aplicativo, se encuentra en estado abierto, debido a la comunicación del servidor con el usuario final, sin embargo, se puede evidenciar una buena práctica del manejo de controles y seguridad de puertos, al no alojar la aplicación en el rango de puertos bien conocidos 1 - 1024, mitigando la posible apertura de brechas de seguridad por medio de exploits a este rango de puertos, al ser la aplicación alojada en un puerto registrado, complica el rastreo de vulnerabilidades para el ciber atacante.

10.1.2 SERVIDOR

10.1.2.1 HERRAMIENTA ANÁLISIS DE SERVIDOR

Nessus, es un programa de escaneo de vulnerabilidades para diversos sistemas operativos comerciales y no comerciales, en el cual consiste en ejecutar el escaneo del sistema objetivo, mostrando a modo de informe, el estado actual de la dirección IP que se evalúa. Esta herramienta

funciona como escáner de puertos e identificación de exploits posibles según la base de conocimiento proporcionada por el mismo instrumento, el cual se utilizó con la versión libre.

10.1.2.2 ANÁLISIS DE SERVIDOR

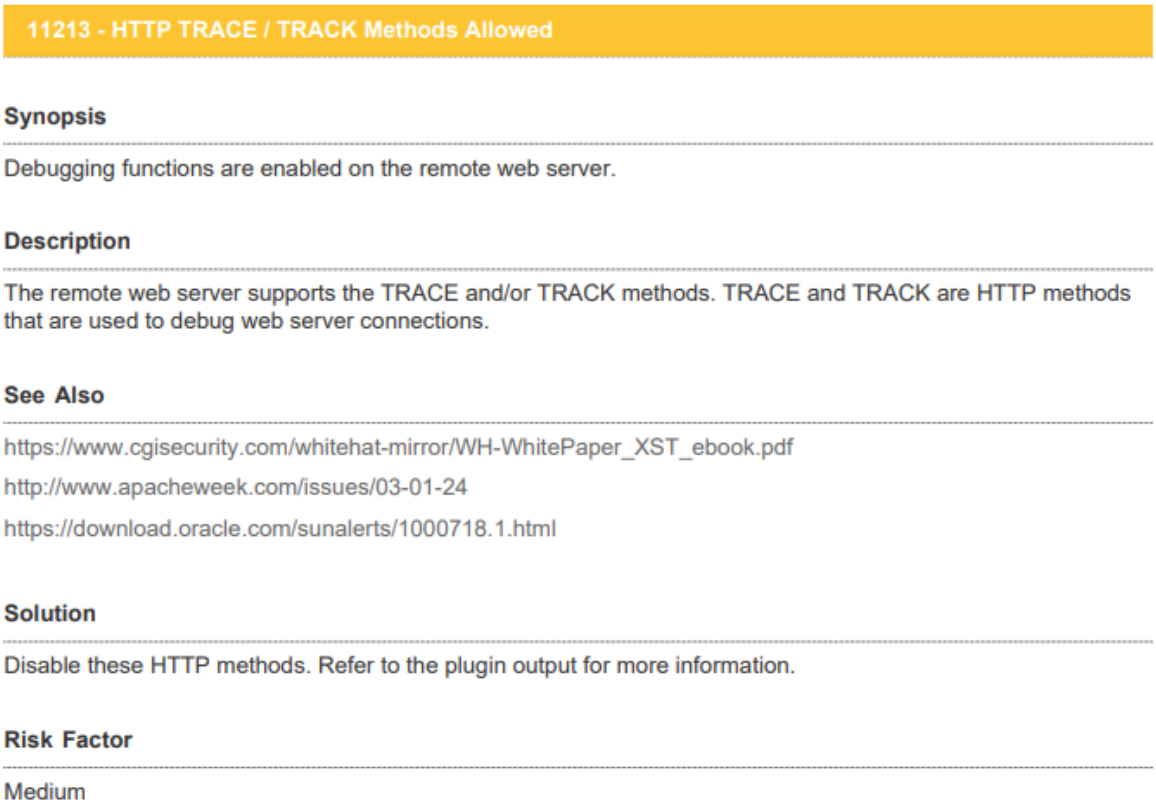

Ilustración 7 Análisis con herramienta Nessus

10.1.2.3 RESULTADOS ANÁLISIS DE SERVIDOR

Se identifica que el servidor web remoto admite los métodos TRACE y/o TRACK. Definidos como métodos HTTP, que se utilizan para depurar las conexiones del servidor web. Estos métodos se utilizan para la entrada de datos de los usuarios web, donde generan las cookies donde se obtiene el enlace de sesión de dicho usuario.

10.1.3 TRÁFICO DE DATOS APLICATIVO WEB

10.1.3.1 HERRAMIENTA ANÁLISIS DE TRÁFICO DE DATOS APLICATIVO WEB

Wireshark, es un instrumento que actúa como analizador de protocolos, utilizado para ejecutar soluciones de identificación de data para cada uno de los protocolos de las diferentes capas de un sistema de comunicación, en este caso, de telecomunicación a nivel de red, útil para la obtención de información del flujo de datos y el accionar de protocolos en una red. Se efectuará el análisis de tráfico del aplicativo web para realizar una posterior identificación de vulnerabilidades a nivel de seguridad.

10.1.3.2 ANÁLISIS DE TRÁFICO DE DATOS APLICATIVO WEB

Ilustración 8 Aplicativo web

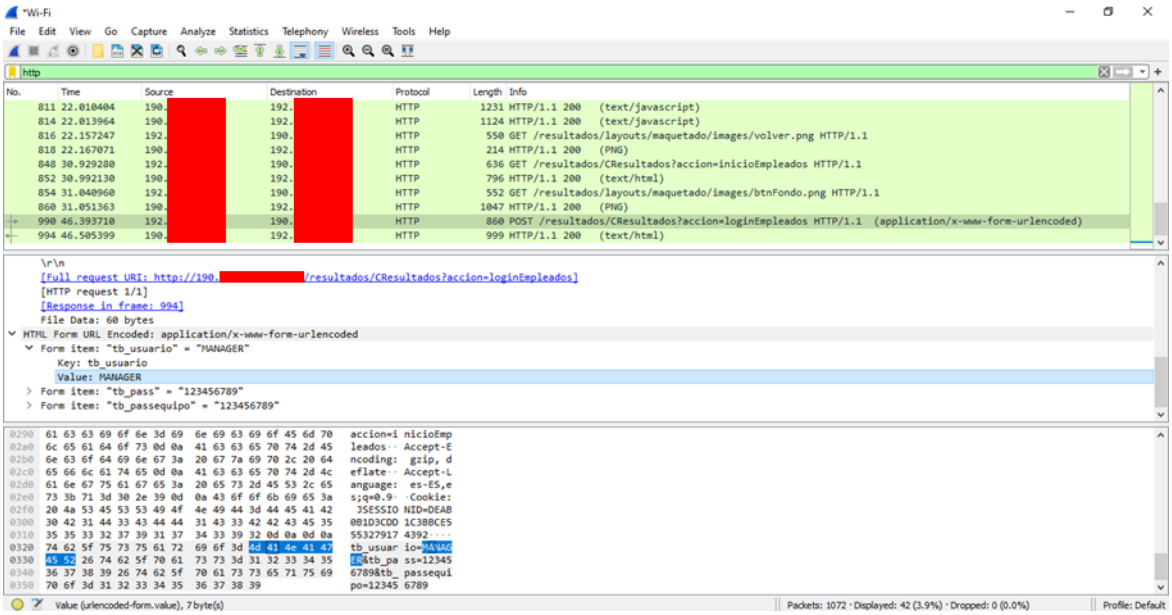

Ilustración 9 Análisis de protocolos con Wireshark

10.1.3.3 RESULTADOS ANALISIS DE TRÁFICO DE DATOS EN APLICATIVO WEB

La página web no cuenta con un sistema de protección de seguridad del tráfico de datos entre origen y destino que permita cifrar la información que viaja por la web. Al no contar con dichos controles en la arquitectura, todos los datos tal como se evidencia en los resultados de la herramienta utilizada, navegan desde el Punto A (Usuario) al Punto B (Laboratorio), en texto plano, lo que permite que presuntos ciberdelincuentes, presencien un escenario a su favor para interceptar usuarios y contraseñas de acceso para la descarga de resultados clínicos de terceros. Obteniendo como resultado la posible vulneración, tanto de la información del paciente como la

confidencialidad de la arquitectura actual.

10.1.4 ARQUITECTURA WEB

10.1.4.1 ANÁLISIS DE ARQUITECTURA WEB

La arquitectura web consta de elementos de comunicación como lo son los equipos de usuario final, en este caso los pacientes externos, los cuales, por medio de navegación por servicios de internet, realizaran la petición al servidor el cual contiene la aplicación web, servidor de aplicaciones y la base de datos junta, con un punto de control de seguridad parametrizado por un firewall, tal como se muestra la siguiente ilustración.

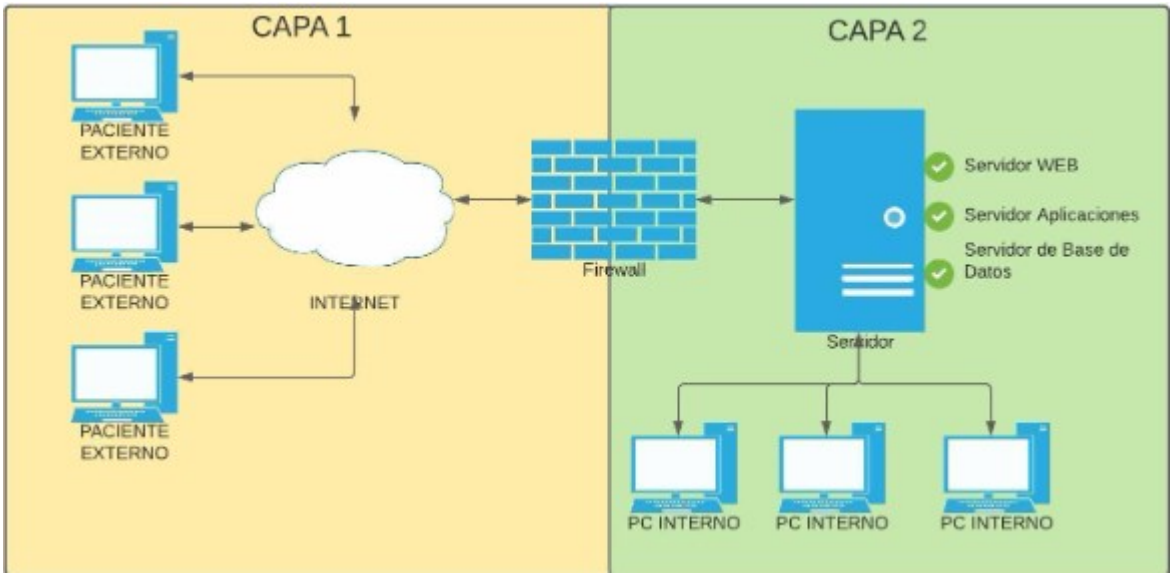

Ilustración 10 Diagrama de arquitectura web

10.1.4.2 RESULTADOS ANALISIS DE ARQUITECTURA WEB

Se cuenta con una arquitectura de 2 capas donde se encuentra el servicio web, la aplicación y la base de datos sin ningún filtro o control de seguridad intermedio entre cada uno de ellos. Por buenas prácticas de seguridad en una arquitectura web, se considera que el servidor web y aplicación deben encontrarse separados del servidor de bases de datos y generar un control para el paso de información de servidor a servidor, incrementando las capas en 3 para el reforzamiento de la seguridad en la arquitectura, así mismo se debe reforzar para garantizar la disponibilidad del servicio un servidor de alta disponibilidad como respaldo, el cual se presente como unidad de backups y contingencia, presente para generación de workaround en caso de que se genere una incidencia ya sea por un posible ataque cibernético, una ventana de mantenimiento o una degradación de los componentes y/o dispositivos pertenecientes a la arquitectura web

Esto se puede identificar en el escaneo de puertos realizado a la IP Pública suministrada donde se encuentra el puerto 5432, ya con esto es claro que se cuenta con una base de datos en el servidor publicado. A este es posible generar un exploit en donde se pueda agregar, modificar

y/o eliminar datos de la misma, generando traumatismo a la integridad de los datos en la misma capa de la aplicación, por lo cual no solo se presentaría la afectación en la disponibilidad de la arquitectura web, sino que también se vería vulnerada la integridad y la confidencialidad de los resultados clínicos a entregar, para con los pacientes, generando un impacto altamente crítico para la organización, arquitectura, proceso y percepción de los acuerdos de nivel de servicio establecidos con el cliente.

A continuación, se presenta la percepción de como seria la propuesta de una arquitectura de tres capas, según las indicaciones, riesgos a mitigar y acciones a realizar para minimizar la brecha de seguridad en la arquitectura web actual.

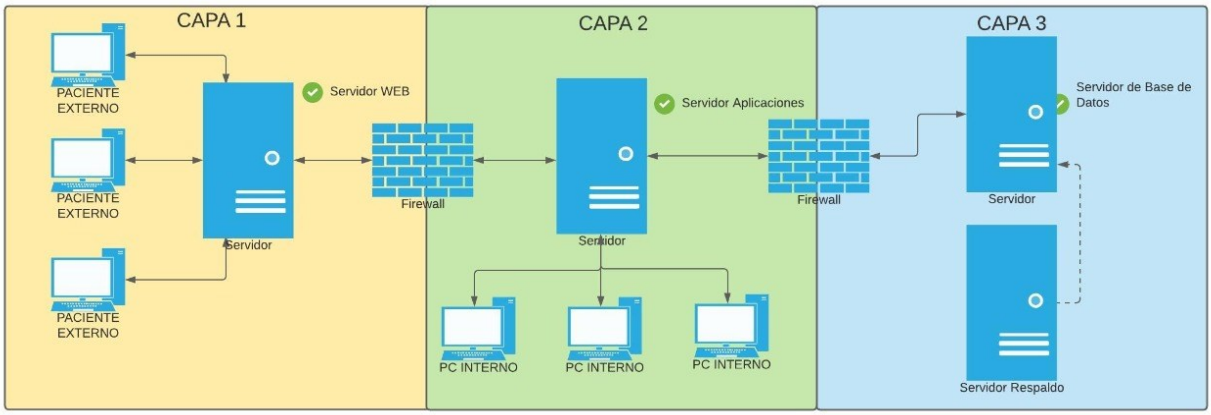

Ilustración 16 Arquitectura web de 3 capas

10.1.5 DNS

10.1.5.1 ANÁLISIS DNS

Ilustración 11 Dirección URL de página web

DNS es un sistema de nombres de dominio el cual traduce las direcciones IP en nombres comunes o legibles para el usuario final, esto con la finalidad de que se pueda referenciar la página web por medios menos técnicos, claro ejemplo de esto es la traducción de uno de los buscadores más conocidos en la actualidad “Google” el cual su dirección IP es 8.8.8.8 y su DNS se representa como www.google.com.

10.1.5.2 RESULTADOS ANÁLISIS DNS

No contar con un DNS Activo en la Dirección IP Pública donde se encuentra el servicio Web.

En este caso en la barra de dirección del navegador donde se haya realizado la búsqueda aparece la IP Pública, con ello genera facilidad al atacante de generar escaneos y descubrir vulnerabilidades de manera más eficiente.

10.2 RIESGOS DE ESTADO ACTUAL DE ARQUITECTURA WEB:

Luego del análisis de cada uno de los componentes de la arquitectura web, se procede a realizar el proceso de gestión de riesgos de cada uno de los componentes analizados, guiado por el siguiente proceso, el cual se describirá sección por sección:

Ilustración 12 Mapa de procesos de gestión de riesgos de estado actual de arquitectura web

10.2.1 VALORACIÓN DE RIESGO

Para valorar riesgos se realiza una matriz de evaluación de probabilidad de probabilidad y valor de impacto, las cuales, comprenden los parámetros siguientes para realizar un análisis cuantitativo que permita obtener el nivel de riesgo al que se encuentra expuesto el activo de información:

PROBABILIDAD	
Alta	>=10
Media	5-9
Baja	<=4

Tabla 2 Evaluación de probabilidad

IMPACTO	
Alta	>=10
Media	5-9
Baja	<=4

Tabla 3 Evaluación de impacto

10.2.2 NIVEL DEL RIESGO

Se establecieron los niveles de riesgos para la organización como se muestra a continuación:

PROBABILIDAD	ALTO	3	6	9
	MEDIO	2	4	6
	BAJO	1	2	3
		BAJO	MEDIO	ALTO
	IMPACTO			

Tabla 4 Matriz de nivel de riesgo

10.2.3 DEFINICIÓN DE RIESGOS

A continuación, se mencionan cada uno de los riesgos identificados bajo el anterior análisis de los componentes de la arquitectura web:

# Riesgo	Riesgo
R1	Si la estructura actual no cuenta con un certificado digital es posible que se genere pérdida de las credenciales por interceptación.
R2	Si se tiene los puertos de la arquitectura abiertos sin ningún control puede generar explotación por parte de un atacante al servidor.
R3	Al contar con una arquitectura de dos capas se identifica de manera más ágil el sistema operativo del servidor
R4	El servidor web remoto admite los métodos TRACE y / o TRACK. TRACE y TRACK son métodos HTTP, que se utilizan para depurar las conexiones del servidor web.

Tabla 5 Definición de riesgos

10.2.4 ANÁLISIS DE LOS RIESGOS

Acorde a lo revisado en las anteriores fases, los riesgos se ponen en proceso de evaluación según los criterios para la identificación del nivel del riesgo a partir de una escala de impacto vs probabilidad, una vez se ejecuta la clasificación de cada uno de los riesgos definidos, se procede a ubicar los mismos en lo que se denomina el mapa de calor de riesgos, en donde nos indica si el riesgo es calificado como bajo, medio o algo. Tal como se ve en la siguiente ilustración, se puede evidenciar que los riesgos R1 y R2 se encuentran ubicados como un riesgo alto, por otro lado, los riesgos R3 y R4 se encuentran ubicados en un nivel de riesgo medio o moderado.

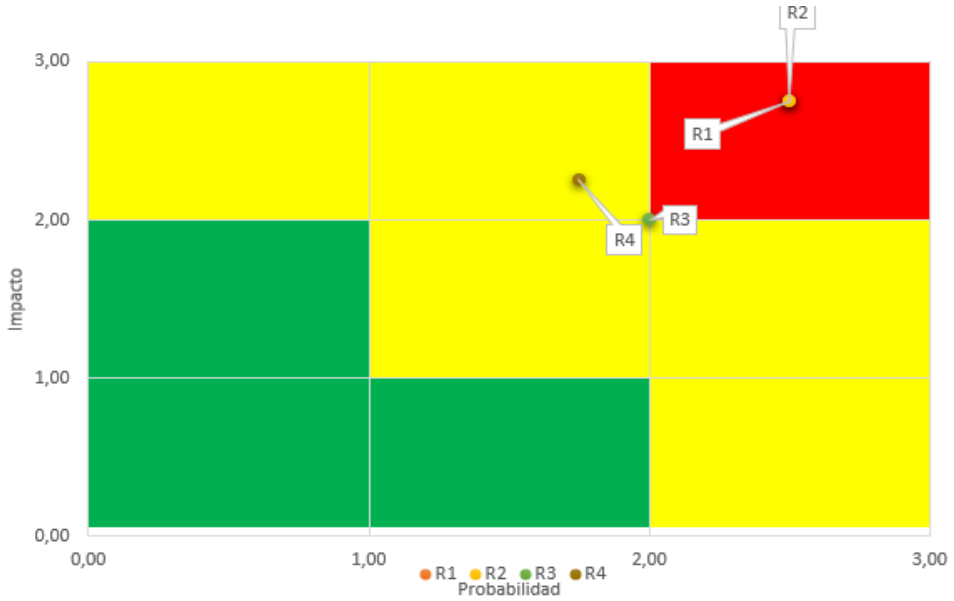

Ilustración 13 Mapa de calor de riesgos

10. MATRIZ DE RIESGOS

Revisar anexo “Matriz de riesgos”.

11. PLAN DE MEJORA

11.1 PROBLEMA

Actualmente la organización no posee los suficientes mecanismos pertinentes en cuanto al control de flujo de información a través de la red, siendo vulnerable a ataques cibernéticos que afecten la información de la organización y/o clientes.

11.1.1 IDENTIFICACIÓN DEL ÁREA DEL PROBLEMA

11.1.1.1 SEGURIDAD TI

La falta de controles de seguridad de la información de entrega de resultados clínicos, genera una brecha para posibles incidencias mayores, que vulneren los datos de clientes y organización.

11.1.1.2 INFRAESTRUCTURA TECNOLÓGICA

Una incidencia de seguridad se puede presentar por entornos no seguros o labores de mantención no ejecutadas a tiempo, como el despliegue de parches y actualizaciones, así como la implementación de buenas prácticas en los dispositivos de seguridad perimetral y asignación correcta de roles y depuración de usuarios periódicamente.

11.1.1.3 DESARROLLO

La ejecución y publicación de código en entorno de producción, sin ser testado anteriormente y avalado, donde se cumplan con los parámetros de seguridad como controles de documentación de código, ofuscación del mismo, entre otros.

11.1.1.4 ADMINISTRACIÓN

Un ciberataque puede paralizar la producción del cliente y/o organización, por lo que las labores administrativas según el caso aumentan en cuestiones de toma de decisiones y se disminuiría en el escenario de que no sea permitido el acceso a dispositivos de almacenamiento ni hardware de la organización.

11.1.1.5 FINANZAS

La pérdida de información de la organización o el cliente, repercute económicamente en pagos de horas extras a personal y posibles adquisiciones por fuera del presupuesto que pueden afectar los procesos planificados por el área.

11.1.1.6 CONTROL INTERNO

Afectación considerable en las métricas a evaluar de cada uno de los procesos debido a las posibles fallas a niveles de tecnología y operación, generando imprecisión del control y seguimiento de procesos.

11.1.1.7 ATENCIÓN AL CLIENTE

Bajo un ciberataque que afecte la información de los clientes, las labores de atención al cliente se verán reflejadas en el aumento de labores y sobrecargo de actividades de atención, con riesgos de pérdida o cancelación de contratos y/o servicios prestados a los entes mencionados.

11.1.1.8 OPERACIONES

Se presentarán afectaciones en el flujo normal de trabajo y la utilización de servicios para el desarrollo de actividades laborales cotidianas en el área, generando retrasos e ineficiencia del trabajo con los recursos asignados.

11.1.1.9 CLIENTE

Se verá perjudicado y perderá credibilidad en la organización siendo un riesgo crítico para la misma, además de que se efectúen posibles acciones legales por no velar por la información del cliente.

11.1.2 DETECCIÓN DE CAUSAS DEL PROBLEMA

- Omisión de controles de seguridad en proceso de entrega de resultados clínicos.
- Desconocimiento de vulnerabilidades publicadas recientemente que puedan ser explotadas.
- No asignación de presupuesto para el proceso de seguridad en entrega de resultados clínicos.
- Cronograma estipulado anual/semestral para el área de Desarrollo el cual no contempla requerimientos del proceso de seguridad en entrega de resultados clínicos.

- Costo elevado en generación de controles de seguridad, que afectan la planeación y presupuesto asignado para la organización.

11.1.3 OBJETIVO DE MEJORA DEL PROBLEMA

Garantizar la integridad y la confidencialidad para el proceso de entrega de resultados de laboratorio clínico a los diferentes roles pertinentes manejados por la organización.

11.2 PROTOCOLO DE ELABORACIÓN DEL PLAN DE MEJORA

A continuación, se presenta la estructura de trabajo para la elaboración del plan de mejora del problema presentado anteriormente:

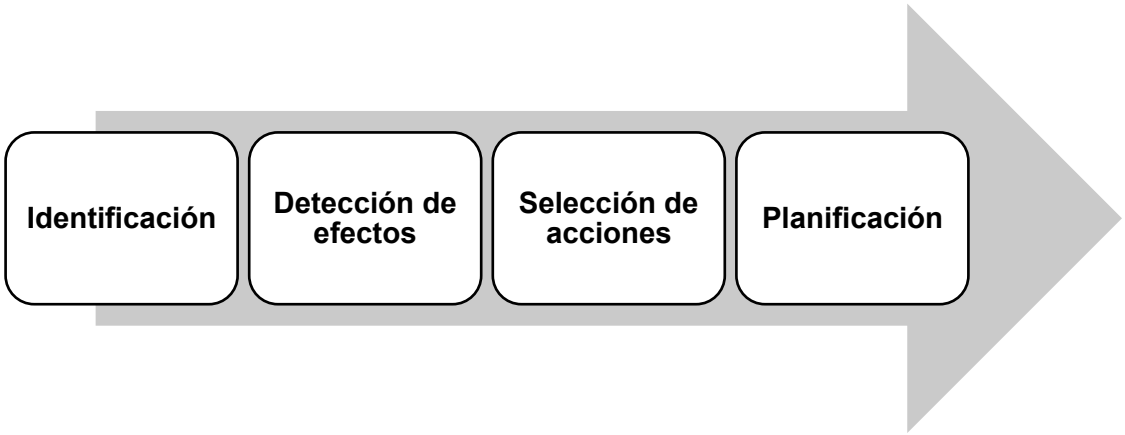

Ilustración 14 Mapa de procesos elaboración plan de mejora

11.2.1 IDENTIFICACIÓN DEL ÁREA DE MEJORA

11.2.1.1 SEGURIDAD TI

Generar controles de seguridad en el proceso de entrega de resultados clínicos disminuirá la brecha y puertas traseras potenciales para evitar ataques cibernéticos.

11.2.1.2 INFRAESTRUCTURA TECNOLÓGICA

Mejora de procesos de gestión de roles y usuarios, así mismo la gestión de actualizaciones y prueba de parches de seguridad de la infraestructura tecnológica.

11.2.1.3 DESARROLLO

Gestión de testeo de desarrollos, requerimientos, entre otros, documentación de los mismos orientados a objetivos funcionales y entornos seguros para perseverar por la información del usuario final.

11.2.1.4 ADMINISTRACIÓN

La mitigación de ciberataques no afectaría las incidencias en el área administrativa, por lo que las labores de cronograma se ejecutarán de manera normal en el proceso, sin generar retrasos o posibles imprevistos en sus actividades laborales.

11.2.1.5 FINANZAS

Reducción de la probabilidad del riesgo, mitigando pérdidas económicas imprevistas en la gestión de activos de la organización.

11.2.1.6 CONTROL INTERNO

Controles efectivos y acertados de las métricas evaluadas por el área para cada uno de los procesos, obteniendo resultados precisos sin afectar los seguimientos pertinentes que se realizan a dichos procesos.

11.2.1.7 ATENCIÓN AL CLIENTE

Reducción de picos de trabajo en actividades de atención al cliente, evitando posibles solicitudes de personal, reduciendo costos de operación y mejorando la calidad del servicio prestado.

11.2.1.8 OPERACIONES

Optimización de flujos de trabajo, aprovechando el uso de recursos para elaboración de actividades laborales en los tiempos estimados.

11.2.1.9 CLIENTE

La percepción de la entrega de resultados clínicos, se verá reflejado positivamente al evidenciar controles de seguridad para la preservación de su información, generando futuras recomendaciones a externos, beneficiando a la organización.

11.2.2 DETECCIÓN DE EFECTOS DE MEJORA

- ✔ Optimización de procesos de operaciones.
- ✔ Atención al público efectiva y eficiente.
- ✔ Entorno seguro y confiable para el cliente.
- ✔ Reducción de riesgos por ataques cibernéticos y vulneración a información de terceros.
- ✔ Mejorar experiencia al cliente para con los servicios suministrados.
- ✔ Agregar valor de calidad de servicio a ofrecer en portafolio de negocios.

11.2.3 ÁREAS DE MEJORA

La evaluación de riesgos identificados parte como principal factor de la selección de acciones de mejora en la organización, identificando por medio de la matriz de análisis de riesgos de seguridad de la arquitectura web del proceso de entrega de resultados clínicos, riesgos los cuales serán evaluados con la finalidad de disminuir la probabilidad y el impacto generados por el mismo.
A continuación, los factores que se identificaron y se catalogaron como aspectos a mejorar:

# Área	Área de mejora
A1	Si la estructura actual no cuenta con un certificado digital es posible que se genere pérdida de las credenciales por interceptación.
A2	Si se tiene los puertos de la arquitectura abiertos sin ningún control puede generar explotación por parte de un atacante al servidor.
A3	Al contar con una arquitectura de dos capas se identifica de manera más ágil el sistema operativo del servidor
A4	El servidor web remoto admite los métodos TRACE y / o TRACK. TRACE y TRACK son métodos HTTP, que se utilizan para depurar las conexiones del servidor web.

Tabla 7 Identificación áreas de mejora

11.2.4 PLANIFICACIÓN DE MEJORA

Área de mejora A1	
Descripción del problema	Si la estructura actual no cuenta con un certificado digital es posible que se genere pérdida de las credenciales por interceptación.
Causas que provocan el problema	• C1. Falta de recursos asignados para la adquisición de un Certificado Digital por medio de un ente certificador • C2. Desconocimiento de las Vulnerabilidades • C3. Pérdida de información por navegación en texto plano • C4. Poco interés de los stakeholders
Objetivo a conseguir	Reducir el riesgo por pérdida de información y vulneración de credenciales por interceptación.
Acciones de mejora	• CTR1 Procedimiento para verificar que el certificado digital esté bien instalado. • CTR2 Chequear la fecha de vencimiento del certificado digital. • CTR3 Capacitación al usuario final. • CTR4 Implantación de una estructura centralizada y segura para el almacenamiento de las claves, basada en un hardware criptográfico HSM. • CTR5 Sólo personal autorizado, debe tener acceso donde se encuentran almacenadas las claves. • CTR6 Verificar que el certificado se encuentre funcionando • CTR7 Presentación de la importancia de un Certificado Digital de manera ágil y concreta a las directivas

Tabla 8 Plan de mejora A1

Área de mejora A2	
Descripción del problema	Si se tiene los puertos de la arquitectura abiertos sin ningún control puede generar explotación por parte de un atacante al servidor.

Causas que provocan el problema	• C1 Capturar el puerto 5432 capturar la Base de Datos y manipular su información • C2 Posibilidad de sniffer • C3 Denegación de Servicio (DoS) • C4 Ataque CGI
Objetivo a conseguir	Proteger la arquitectura web, evitando ataques cibernéticos al servidor por medio de explotación de puertos.
Acciones de mejora	• CTR1 Utiliza puertos que no sean un estándar. • CTR2 Abre exclusivamente los puertos necesarios. • CTR3 Usar métodos preventivos: Cortafuegos e IDS. • CTR4 Actualizaciones: Mantenga los servicios siempre actualizados. • CTR5 Ocultar información. Desactivar los banners de información de cualquier servicio. • CTR6 Capacitar al personal para instalar de manera efectiva y correcta una arquitectura de tres capas • CTR7 Encriptación de datos

Tabla 9 Plan de mejora A2

Área de mejora A3	
Descripción del problema	Al contar con una arquitectura de dos capas se identifica de manera más ágil el sistema operativo del servidor
Causas que provocan el problema	• C1. Ingreso de Usuarios no autorizados • C2. Falta de Control de la aplicación a la Base de Datos • C3. Servidor centralizado • C4. Falta de Capacidad para el manejo de la Información • C5. Implementaciones con bajo presupuesto
Objetivo a conseguir	Modelo de arquitectura segura para reducir identificación de sistema operativo del servidor a ciberdelincuentes
Acciones de mejora	• CTR1 Actualizaciones: Mantenga los sistemas operativos siempre actualizados. • CTR2 Implementar un cortafuegos de aplicaciones web (WAF). • CTR3 Endurecimiento del sistema Hardening. • CTR4 Limitar la cantidad de información sensible almacenada en bases de datos accedidas por aplicaciones web al mínimo necesario y protegerla mediante cifrado. • CTR5 Implementando CAPTCHA o incitando a los usuarios a responder preguntas. Esto asegura que un formulario y una solicitud sean enviados por un humano y no por un bot. • CTR6 Backups de manera diaria de la información y arquitectura. • CTR7 Capacitación al personal • CTR8 Planificación de mejora. • CTR9 Reducción de la probabilidad del riesgo, mitigando pérdidas económicas imprevistas en la gestión de activos de la organización.

Tabla 10 Plan de mejora A3

Área de mejora A4	
Descripción del problema	El servidor web remoto admite los métodos TRACE y / o TRACK. TRACE y TRACK son métodos HTTP, que se utilizan para depurar las conexiones del servidor web.
Causas que provocan el problema	• C1. Navegación en texto plano • C2. Un usuario local o remoto sin privilegios puede secuestrar las funcionalidades • C3. Solicitudes maliciosas • C4. Permite el acceso no autorizado
Objetivo a conseguir	Restringir la admisión de métodos TRACE y/o TRACK.
Acciones de mejora	• CTR1 Deshabilite estos métodos HTTP. • CTR2 Verificar que el certificado SSL del servidor no haya expirado. • CTR3 Actualizaciones: Mantenga el servicio de Apache siempre actualizados. • CTR4 Implementando CAPTCHA. • CTR5 Establecer un timeout de sesión. • CTR6 Seguimiento al tráfico entrante • CTR7 Validación de LOGS de auditoría

Tabla 11 Plan de mejora A4

12. RESULTADOS

Acorde a los objetivos y los respectivos requerimientos y entregables del proyecto, se realiza la entrega y análisis de resultados de cada uno de los tangibles del proyecto en mención.

- Documento estado actual de integridad y confidencialidad de la información en la entrega de resultados clínicos.

La primera fase de Análisis el cual se centraba en el levantamiento de la información en lo que respecta a los aspectos técnicos y de operación que se presentaban en el mapa de procesos del funcionamiento normal de la herramienta y de su actividad en cuanto a labores de seguridad de la información en cada uno de estos procesos, recopilando información clave a evaluar bajo los conocimientos adquiridos a lo largo de la experiencia en la especialización en seguridad de redes telemáticas, junto con el valor agregado de cada uno de los ingenieros partícipes del proyecto, que por sus habilidades se logra realizar el respectivo análisis del estado actual de la seguridad de la arquitectura web para la entrega de resultados clínicos a pacientes y/o clientes.

- Matriz de riesgos para analizar las vulnerabilidades del proceso de entrega de resultados clínicos a pacientes y/o clientes de la organización.

Para la segunda fase se enfoca en la identificación de los puntos claves los cuales son pertenecientes a los aspectos de evaluación de vulnerabilidades y riesgos de la arquitectura web, es preciso realizar la identificación de dichos factores para centrarse en el alcance del proyecto, por esta razón se realiza una matriz de vulnerabilidades que permite masificar la data en ambientes controlados y de gestión bajo aplicativos ofimáticos para su eficiencia al momento de evaluar la información analizada e identificada, para que así mismo sea cuantificada.

- Documento propuesto de mejora de seguridad para la integridad y confidencialidad en la entrega de resultados clínicos.

La documentación de un proceso de mejora debe ir soportado de una respectiva identificación de riesgos del proceso, por lo que se procede a realizar la evaluación de cada uno de los ítems y cercar el alcance de cada uno de estos, para generar una solución íntegra y que cubra con un gran porcentaje de la seguridad de la información en lo que respecta a dicho proceso, para mantener la credibilidad de los clientes y darle un plus del tratamiento de sus datos personales, garantizando la integridad y confidencialidad en el proceso.

- Formato de requerimientos necesarios para ampliar la confidencialidad e integralidad de la información emitida en los PDF por la arquitectura actual.

Para la consolidación de la información analizada, identificada y evaluada, es preciso realizar un requerimiento técnico para el área de TI, bajo el formato especificado por las directrices de la organización, requerimiento que ingresa al banco de requerimientos a evaluar, estos son puestos a revisión por el director de TI el cual indicará si el proyecto es o no viable para la organización, el alcance de este proyecto se ubica en la generación de un requerimiento técnico soportado por bases de identificación de la información analizada a lo largo del proyecto.

13. DISCUSIÓN

Se pueden evidenciar 4 aspectos críticos, a los cuales se les proporcionó, por medio de las herramientas pertinentes de análisis de seguridad, el proceso de evaluación de riesgos obteniendo el siguiente análisis por mapa de calor del riesgo inherente y residual, el análisis de resultados de cada uno de los riesgos trabajados.

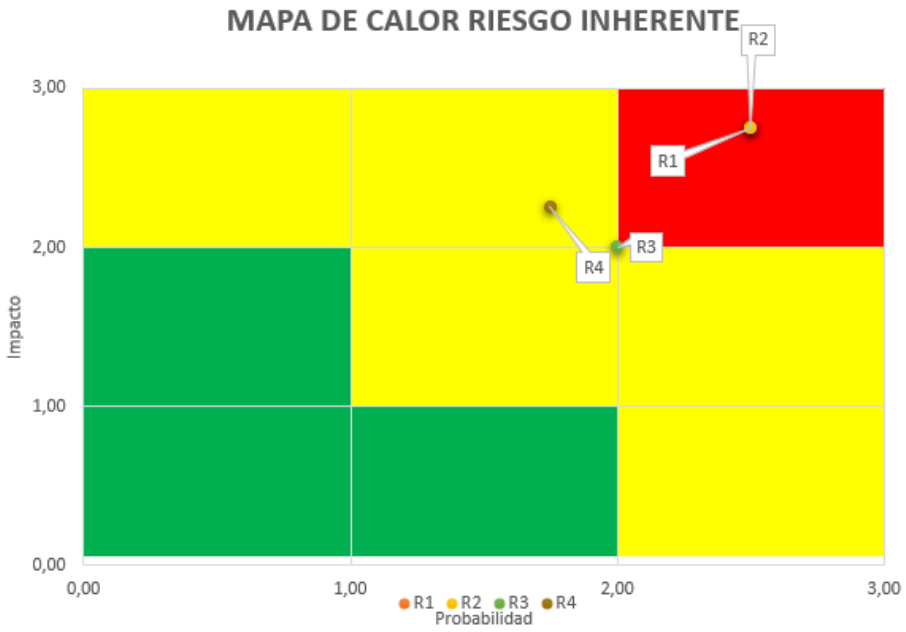

Ilustración 15 Mapa de calor riesgo inherente

- R1: Se puede evidenciar que la arquitectura web actual, no cuenta con un certificado digital, esto a causa de causales como falta de recursos asignados para la adquisición de un ente certificador, el desconocimiento de porqué un certificado digital es indispensable para garantizar la seguridad de la información transmitida, por medio de interceptación de información en texto plano, lo que ocasiona impactos de carácter critico tales como la vulneración de la información de los resultados clínicos, por lo que es recomendable la implementación de controles que mitiguen el riesgo por medio de la adquisición de un certificado digital, capacitación o jornadas de sensibilización con el usuario final en temas de seguridad de la información y la implementación de una arquitectura segura para perseverar la integridad y confidencialidad del proceso de entrega de resultados clínico, reduciendo el nivel de impacto vs probabilidad de alto a medio-bajo.
- R2: En el estado actual de la arquitectura web, se presentan puertos en estado abierto sin ningún control de seguridad, por lo que puede ser una brecha para posibles explotaciones de vulnerabilidades por parte de ciberdelincuentes, esto causado por la identificación de puertos como 5432 exponiendo servicios como bases de datos, o posibles ataques CGI o DoS, afectando la disponibilidad del proceso de entrega de resultados clínicos, por lo tanto la aplicabilidad de controles como el cambio de puertos para los servicios para evitar la utilización de puertos por defecto o conocidos, el uso de únicamente los puertos requeridos para la prestación del servicio, controlados por servidores de seguridad perimetral tales como firewall e IDS, se podrá reducir el impacto vs probabilidad del riesgo

de un estado alto a un valor medio.

- R3: Una arquitectura web de dos capas disminuye el tiempo de identificación del sistema operativo del servidor, a causa de falta de controles de aplicativos como la base de datos y la exposición de servidores para accesos de usuarios no autorizados, dejando en evidencia las capacidades para el correcto manejo de la información en el proceso de entrega de resultados clínicos, lo cual puede generar la vulneración de la confidencialidad de los datos de los pacientes y organización, así mismo se vería afectada la disponibilidad del servicio en caso de que el servidor sufra un ataque cibernético, aumentando tiempos de implementación y restauración de servicios generando perdidas y confianza en los clientes, por lo que para la mitigación de dichos sucesos, la constante actualización de parches de seguridad en sistemas operativos, implementación de dispositivos perimetrales (WAF) Web aplicación firewall, realizar validaciones de Hardering y limitar el almacenamiento de información sensible en bases de datos a las cuales se acceden por aplicaciones web, así mismo la implementación de CAPTCHA como doble factor de autenticación de usuario, reducirán la probabilidad del riesgo, así mismo con la separación de servicios y servidores, incluyendo una contingencia para perseverar la alta disponibilidad del servicio, funcionando como controles de seguridad perimetral, mitigando pérdidas económicas no contempladas en la gestión de activos de la organización, obteniendo un impacto vs probabilidad de nivel alto a medio.

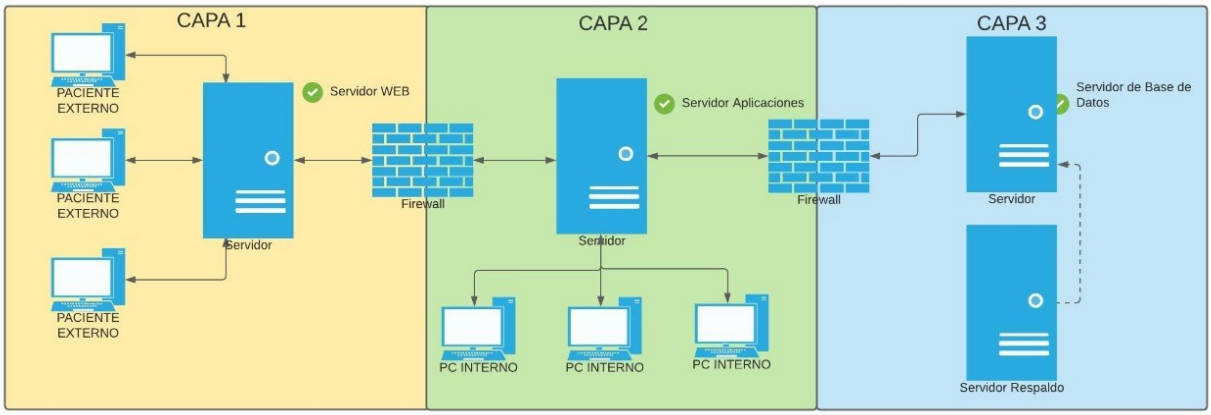

Ilustración 16 Arquitectura web de 3 capas

- R4: El servidor web remoto, al permitir los métodos TRACE y/o TRACK, los cuales se utilizan para la depuración de conexiones del servidor, causan posibles solicitudes externas o de accesos no autorizados, así como la navegación por medio de texto plano de usuarios locales o remotos sin privilegios que potencialmente pueden ejecutar ataques

al servidor, accediendo y vulnerando la confidencialidad e integridad por medio de captura de información por la red, así como la obtención de acceso a los encabezados HTTP de la aplicación afectando la integridad del servidor, el cual por medio de controles como la deshabilitación de los métodos mencionados, la verificación del certificado SSL del servidor en estado vigente, la actualización del servicio web y el seguimiento de logs reducirán presuntos ataques informáticos, mitigando el riesgo de un nivel de impacto vs probabilidad medio-alto a un nivel medio-bajo.

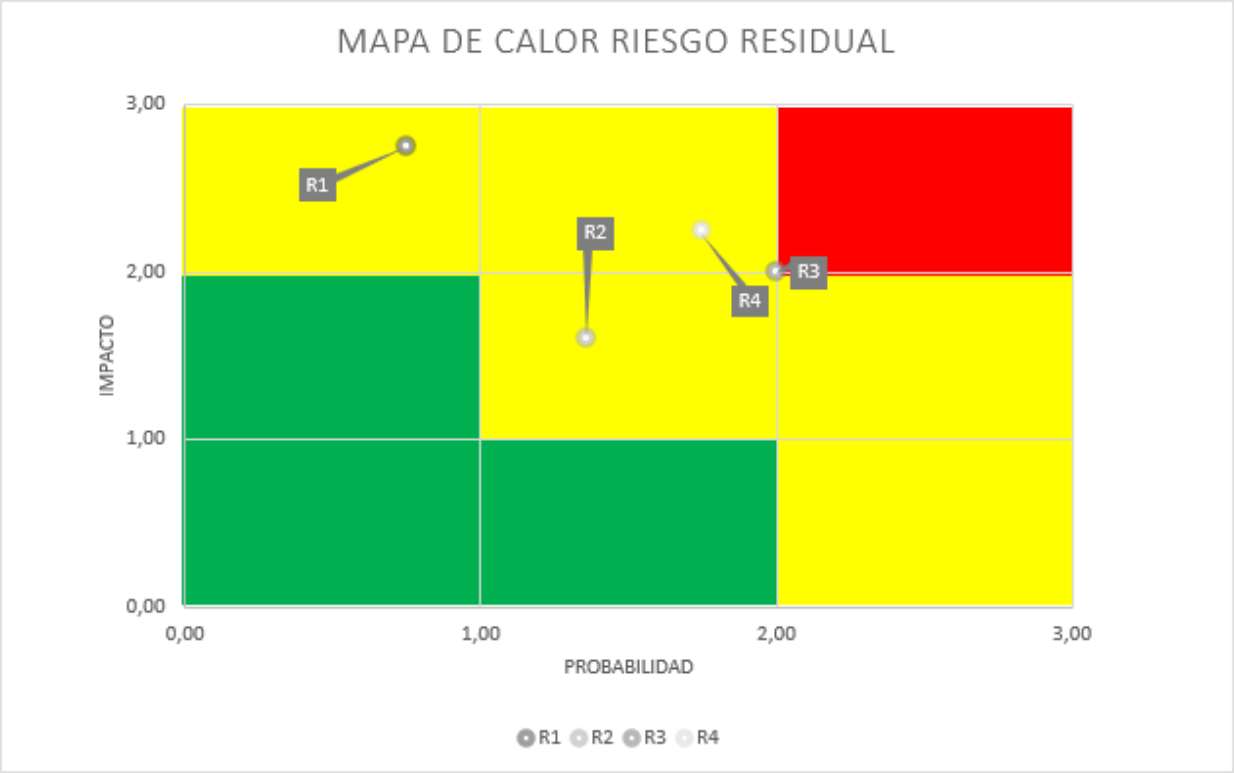

Ilustración 17 Mapa de calor riesgo residual

14. CONCLUSIONES

- ✔ Un análisis de riesgos y vulnerabilidades parte de una previa identificación del estado actual del proceso a revisar, por ende, dicha identificación debe ser oportuna y precisa para enfocarse en lo que se requiere evaluar, apoyándose con herramientas de análisis de seguridad que ayudan al especialista a detectar el panorama, filosofía y entorno en el cual se encuentra, para ejecutar un proceso de evaluación acertado y efectivo.
- ✔ El primer paso en la cadena de un ciber ataque es la identificación del objetivo, lo cual por medio de diferentes herramientas de uso libre, es de fácil acceso para

mencionado objetivo, uno de los escaneos más comunes para la detección de vulnerabilidades, son los escaneos de puertos, donde se evidencia el estado y los puertos que se utilizan en el servidor y como impactan la arquitectura web, por lo que es de suma importancia mantener al margen el mínimo de puertos abiertos y debidamente controlados en seguridad perimetral y uso de puertos registrados y no bien conocidos. Esto para mitigar la brecha de seguridad y reducción del impacto del riesgo que vulnere la integridad, confidencialidad y disponibilidad de la arquitectura web para la entrega de resultados clínicos.

- ✔ Una arquitectura web de dos capas, bajo el esquema de servidor cliente, a nivel funcional es pertinente para la eficiencia del proceso de entrega de resultados clínicos, sin embargo, al no presentar un plan de contingencia, por indisponibilidad bajo incidencias o eventos programados en el único servidor de la arquitectura web, aumenta la brecha de riesgo en la arquitectura en cuanto a la preservación de la alta disponibilidad del aplicativo, vulnerando la disponibilidad del servicio y al tener alojados los servicios de base de datos, también se ve perjudicado la integridad y confidencialidad de los resultados clínicos, es por esto que una arquitectura de tres capas, refuerza los controles de seguridad perimetrales, mitigando riesgos en cuanto a la prestación y calidad del servicio para con los usuarios finales y su entrega oportuna, eficiente y bajo un esquema de seguridad robusto, que protege la información sensible del mismo.
- ✔ La identificación de riesgos a partir del conocimiento del componente a evaluar, en este caso la arquitectura web, es pilar fundamental como referencia de punto de partida para la identificación del riesgo, las causas por las cuales se presenta este, el impacto originado por el mismo y así mismo las acciones de mejora o controles que posteriormente propuestos, por medio de una matriz de evaluación, cuantifican el estado actual y el valor futuro de lo que generan los controles, con la finalidad de perseverar por la integridad, disponibilidad y confidencialidad de la información tanto de la organización, como de los pacientes debido a que el proceso evaluado involucra stakeholders internos y externos, causando un impacto positivo para ambas partes.
- ✔ El diseño de una propuesta de mejora para este proyecto se presenta como el esfuerzo del levantamiento de información por medio de herramientas de seguridad evidenciados a lo largo de la especialización, las cuales permitieron el análisis y posterior generación de instrumentos de cuantificación de riesgos por

medio de matrices estructuradas, asociadas a un estudio de impacto vs probabilidad generando mapas de calor y parámetros evaluativos, los cuales identifican la criticidad de un riesgo y la toma de decisiones a partir de la generación de controles que reducen el impacto de un riesgo inherente, para obtener un riesgo residual el cual por medio de un proceso iterativo y de evolución periódico, la brecha de riesgo en aspectos de seguridad de la información será reducida considerablemente, garantizando la disponibilidad del proceso de entrega de resultados clínicos, asegurando la confidencialidad para el proceso y seguridad de la información transmitida y brindando confianza a través de la integridad de la información, la cual será verídica y certificada para mayor seguridad del paciente al momento de recibir los resultados clínicos emitidos por la arquitectura web de la organización.

15. DOCUMENTACIÓN DE REFERENCIA

1. Autores: Camara Colombiana de Informatica y Telecomunicaciones. Publicado: 21 abril del 2020
   Definición: CCIT.
   https://www.ccit.org.co/noticias/aumento-37-la-ciberdelincuencia-en-colombia-relacionada-con-el-covid-19/
2. Autores: Julián Pérez Porto y Ana Gardey. Publicado: 2010. Actualizado: 2013.
   Definición: Definición de confidencialidad.
   https://definicion.de/confidencialidad/
3. Autores: Julián Pérez Porto y María Merino. Publicado: 2008. Actualizado: 2012.
   Definición: Definición de integridad.
   https://definicion.de/integridad/
4. Autores: Infoguia. Publicado: 22 de septiembre del 2014, Infoguia.
   Definición: Laboratorio Clínico.
   https://infoguia.com/infotip.asp?t=que-es-un-laboratorio-clinico&a=75
5. Autores: Javier Júdeza, Pilar Nicolásb, M. Teresa Delgadoc, Pablo Hernandod, José Zarcoe y Silvia Granollersf para el Proyecto de Bioética para Clínicos del Instituto de Bioética de la Fundación de Ciencias de la Salud. Publicado: 19/03/2017.
   Definición: Historia clínica.
   http://www.elsevier.es
6. Autores: Julián Pérez Porto y María Merino. Publicado: 2010. Actualizado: 2013.

Definiciones: Definición de web.
https://definicion.de/web/

7. Autores: HostingPedia. Publicado: 2 de junio 2017. HostingPedia
   Definición: Sistema Operativo CentOS.
   https://hostingpedia.net/centos-linux.html
8. Autores: AJBD Soft. Publicado: 2012
   Definición: Apache Tomcat.
   https://www.ajpdsoft.com/modules.php?name=Encyclopedia&op=content&tid=769
9. Autores: Iván Ramírez. Publicado: 25 julio 2016. Actualizado: 31 enero 2020.
   Definición de Máquina Virtual.
   https://www.xataka.com/especiales/maquinas-virtuales-que-son-como-funcionan-y-como-utilizarlas
10. Autores: Yúbal FM. Publicado: 28 octubre 2019.
    Definición: Memoria RAM.
    https://www.xataka.com/basics/memoria-ram-que-sirve-como-mirar-cuanta-tiene-tu-ordenador-movil
11. Autores: MCPRO. Publicado: 8 mayo 2020
    Definición: Procesador Core
    https://www.muycomputerpro.com/movilidad-profesional/2016/05/20/intel-core/
12. Autores: Julián Pérez Porto y Ana Gardey. Publicado: 2009. Actualizado: 2012
    Definición: PDF. (7 de mayo 2020), Definicón.DE.
    https://definicion.de/pdf/
13. Autores: Javier Júdeza, Pilar Nicolásb, M. Teresa Delgadoc, Pablo Hernandod, José Zarcoe y Silvia Granollersf para el Proyecto de Bioética para Clínicos del Instituto de Bioética de la Fundación de Ciencias de la Salud. Publicado: 19/03/2017.
    Definición: Paciente.
    http://www.elsevier.es

16. ANEXOS

- Análisis detallado de Nessus
- Documento estado actual arquitectura web
- Matriz de riesgos
- Plan de mejora
- Formato necesidades del cliente