APLICACIÓN DE LA METODOLOGÍA PTES EN LA CLÍNICA MEDELLÍN PARA LA IDENTIFICACIÓN DE VULNERABILIDADES EN HISTORIA CLÍNICA ELECTRÓNICA

NATALIA BOISSON MORALES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MEDELLÍN
2020

APLICACIÓN DE LA METODOLOGÍA PTES EN LA CLÍNICA MEDELLÍN PARA LA IDENTIFICACIÓN DE VULNERABILIDADES EN HISTORIA CLÍNICA ELECTRÓNICA

NATALIA BOISSON MORALES

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

Edgar Roberto Dulce
Tutor de Curso
Daniel Felipe Palomo Luna
Asesor

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MEDELLÍN
2020

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Medellín, Fecha sustentación

DEDICATORIA

Con amor dedico este trabajo a mi mamá, mi esposo y mi hijo, que son mis pilares para no rendirme ante ninguna dificultad, con su apoyo y comprensión me acompañan en cada etapa vivida, colaborándome en todo momento y permitirme una entrega más 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.

TABLA DE CONTENIDO

pág.

LISTA DE ILUSTRACIONES

pág.

LISTA DE CUADROS

pág.

GLOSARIO

ANÁLISIS: exploración detallado y profundo de algo en específico para reconocer sus características y sacar conclusiones.

CVE: estandarización del nombre de las vulnerabilidades y exposiciones de la seguridad de la información.

HCE: historia clínica electrónica.

HERRAMIENTA: software utilizado para realizar un trabajo determinado.

INTRUSIÓN: ingresar a un sistema en busca de vulnerabilidades.

METODOLOGÍA: conjunto de métodos y pasos que se deben seguir para un tema determinado.

NAT: traductor de direcciones de red.

PENTESTING: explotar un sistema informático para identificar las vulnerabilidades o fallos que existen y prevenir ataques externos.

PTES: estándar de ejecución de pruebas de penetración.

VLAN: red lógica independiente dentro de la misma red física.

VPN: red privada virtual para conectar una o mas computadoras a una red privada utilizando internet.

VULNERABILIDAD: debilidad presente en un sistema operativo, software o sistema que le permite a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

RESUMEN

Con el avance acelerado de la tecnología y la explotación a las vulnerabilidades presentes en los sistemas informáticos, es necesario implementar metodologías de seguridad y herramientas de análisis que protejan y fortalezcan los sistemas que procesan o almacenen información sensible. También es importante conocer que se protege, que le puede afectar y como se puede defender, antes de iniciar o implementar alguna de esas metodologías.

Al identificar las vulnerabilidades existentes en los dispositivos de red, bases de datos y servidores que hacen parte de la historia clínica electrónica de la Clínica, basado en la metodología PTES, con ayuda de la herramienta Nessus y por medio del método de análisis cualitativo que arroja datos de tipo descriptivo se espera, establecer las vías de ataque disponibles para la aplicación de historia clínica electrónica según los planes de contingencia, el equipo técnico, la infraestructura de red y la seguridad de la Clínica, generar un análisis de vulnerabilidades de la aplicación de historia clínica electrónica a través de una herramienta de seguridad informática, clasificar las vulnerabilidades encontradas en la aplicación de historia clínica electrónica y categorizar esas vulnerabilidades según su nivel de criticidad.

ABSTRACT

With the accelerated advancement of technology and the exploitation of vulnerabilities present in computer systems, it is necessary to implement security methodologies and analysis tools that protect and strengthen systems that process or store sensitive information. It is also important to know what is protected, what can affect it and how it can be defended, before starting or implementing any of these methodologies.

When identifying the existing vulnerabilities in the network devices that are part of the electronic medical record of the Clinic, based on the PTES methodology, with the help of the Nessus tool and through the qualitative analysis method that yields descriptive data, hopes, to establish the attack routes available for the application of electronic medical record according to the contingency plans, the technical team, the network infrastructure and the security of the Clinic, to generate a vulnerability analysis of the electronic medical record application to Using a computer security tool, classify the vulnerabilities found in the electronic medical record application and categorize those vulnerabilities according to their level of criticality.

INTRODUCCIÓN

Las entidades del sector salud procesan, almacenan y transmiten información de los pacientes y por esta razón están obligados a cumplir con normas que acrediten un entorno seguro para el procesamiento de datos confidenciales.

Actualmente la Clínica Medellín no cuenta con una metodología para auditar la seguridad en los dispositivos de red que hacen parte de la historia clínica electrónica y que contiene datos sensibles de sus pacientes, por esta razón surge la necesidad de aplicar la metodología PTES para minimizar los riesgos y sea confiable la transmisión y almacenamiento de la información.

Debido a los múltiples ataques informáticos que ha sufrido este sector y el impacto que generan a nivel económico, social y estructural, se hace necesario implementar una metodología que audite la seguridad en los dispositivos de red que hacen parte de la historia clínica electrónica y que contiene datos sensibles de sus pacientes y la aplicación de una herramienta que permita el análisis de vulnerabilidades existentes, con el fin de tomar las acciones necesarias para que estas no sean explotadas por personas malintencionadas.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Los responsables de la seguridad informática dentro de una organización tienen la única misión de proteger y mantener la red lo más segura posible para garantizar el correcto procesamiento de los datos y minimizar las vulnerabilidades que puedan comprometer la integridad, disponibilidad y confidencialidad de la información.

Para defender los sistemas informáticos es importante realizar un estudio sobre los activos de la organización para descubrir las vulnerabilidades que existen y tomar las acciones necesarias.

Por otra parte, se debe tener claro a qué tipo de personas y ataques puede estar expuesta la organización, porque de acuerdo con el *core* del negocio existen diferentes adversarios y formas de ataque.

Cuadro 1. Adversarios y ataques.

	Cibercriminales	**Competidores y Ciberespionaje**	**Hacktivistas**
¿Por qué?	Beneficio económico	Ventaja sobre la empresa	Expresión de ideas o desacreditar y dañar al oponente
Activos afectados	Tarjetas o datos financieros, información personal y credenciales de usuarios	Propiedad intelectual, información de la empresa, datos confidenciales y credenciales de usuarios	credenciales de usuarios
Tipo de ataque	*Malware*, *Phising*, *Botnets*, Ingeniería social, entre otros.	*Malware*, *Phising*, *Botnets*, Ingeniería social, entre otros.	*Malware*, *Phising*, DDos, Ingeniería social, entre otros.

Fuente: elaboración propia

Existen muchos factores por los que el sector salud se enfrenta a estos ataques, como principal motivo es la extracción de información íntima y confidencial de los pacientes.

A continuación, se puede observar noticias y estadísticas acerca de ciberataques, como, por ejemplo, “Ciberataque al sistema informático de los hospitales en España por medio de un *ransomware* en correos electrónicos, con un mensaje acerca sobre el virus Covid 19, que al dar clic encriptan la información y solicitan dinero para recuperarla”.[1]

También se puede observar esta noticia acerca del descubrimiento por parte de un experto en ciberseguridad, de una base de datos (MongoDB) que se encontraba pública en internet sin ningún tipo de protección o restricción y contenía información confidencial de más de dos millones de pacientes. El experto notificó a los responsables y estos analizaron que presentaba configuraciones por defecto y aseguraron la base de datos a las pocas horas. No es claro cuánto tiempo estuvo sin protección, pero si es claro que muchos ciberdelincuentes se aprovecharon para extraer datos e información sensible. [2]

Otra importante noticia es el *ransomware* que secuestró los dispositivos electrónicos del hospital universitario de Brno, la segunda mayor ciudad de la República Checa, el ataque obligo a cancelar cirugías urgentes y traslados importantes para la salud de los pacientes. Todo esto debido a las VPN implementadas para el trabajo remoto a consecuencia de la pandemia del coronavirus. [3]

Las estadísticas no mienten, y es notable como el sector salud hoy y siempre ha estado en el ojo de los ciberdelincuentes, ya sea para extraer información confidencial como para obtener beneficios económicos.

---

[1] EL PAIS ESPAÑA. La policía detecta un ciberataque al sistema informático de los hospitales. [Sitio web]. España: EL PAIS. [Consulta: 23 de marzo 2020]. Disponible en: https://elpais.com/espana/2020-03-23/la-policia-detecta-un-ataque-masivo-al-sistema-informatico-de-los-hospitales.html

[2] WELIVESECURITY. Datos personales de más de 2 millones de pacientes expuestos en Internet. [Sitio web]. Mexico: Harán, Juan Manuel. [Consulta: 23 de marzo 2020]. Disponible en: https://www.welivesecurity.com/la-es/2018/08/07/datos-personales-pacientes-mexico-expuestos-internet/

[3] ABC SOFTWARE. Los riesgos de un ciberataque a los hospitales durante la pandemia de coronavirus. [Sitio web]. Republica checa: Alonso, Rodrigo. [Consulta: 23 de marzo 2020]. Disponible en: https://www.abc.es/tecnologia/informatica/software/abci-riesgos-ciberataque-hospitales-durante-pandemia-coronavirus-202003190858_noticia.html

Fortinet ha publicado un estudio que revela que Colombia entre abril y julio de 2020 fue el país con más altos niveles de intentos de ataques cibernéticos, con más de 42 billones de intentos de intrusión a los sistemas informáticos.[4]

La mayoría de estos intentos de ataques son llamados *exploits* (códigos o programas que aprovechan las vulnerabilidades de los sistemas o las aplicaciones, para ser controladas por el atacante), estos no generan código malicioso, pero si permiten que los cibercriminales ingresen a los sistemas informáticos.

También son utilizados los *malware* troyanos, que infectan por medio de ingeniería social en correos electrónicos o páginas de interés, al descargar un archivo infectado. Esta técnica por medio del correo electrónico es la puerta de entrada más frecuente de los malware.

El phishing es el ataque más utilizado y su método de infección es por medio de un mensaje, haciéndose pasar por alguien que no es y así acceder a datos personales confidenciales y sensibles.[5]

También la fiscalía y la policía reportan que cada año el cibercrimen en Colombia aumenta, solo en 2019 fueron registrados 28.827 de los cuales el 57% que equivale a 15.948 son infracciones a la ley 1273 de 2009, en segundo lugar, se encuentra la violación de datos personales con 8.037 casos, el tercer lugar es el acceso abusivo a los sistemas informáticos con 7.994 casos y en cuarto lugar el uso de software malicioso con 2.387 casos. [6]

Las principales ciudades de Colombia afectadas por el cibercrimen son:

- Bogotá con 5.308 casos.
- Cali con 1.190 casos.
- Medellín con 1186 casos.

[4] EL TIEMPO. Colombia sufrió 42 billones de intentos de ciberataques en 3 meses. [Sitio web]. Colombia: Fortinet. [Consulta: 23 de marzo 2020]. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/colombia-sufrio-42-billones-de-intentos-de-ciberataques-en-3-meses-413666

[5] DINERO. En solo tres meses Colombia sufrió 42 billones de intentos de ataques cibernéticos [Sitio web]. Colombia. [Consulta 23 de marzo 2020]. Disponible en: https://www.dinero.com/actualidad/articulo/cuantos-ataques-ciberneticos-recibe-colombia/276556

[6] CCIT.ORG. Informe de las tendencias del cibercrimen en Colombia (2019-2020). [Sitio web]. Colombia:[Consulta: 23 de marzo 2020]. Disponible en https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

- Barranquilla con 648 casos.
- Bucaramanga con 397 casos.

Los principales vectores de engaño son:

- Correos fraudulentos personalizados (*Spear Phising*), con el 80%
- Suplantación de identidad, con el 60 %
- Enmascaramiento de correos (*Spoofing*), con el 53%
- Infección de sitios web frecuentemente visitados, con el 37%

Los principales vectores de un ataque *ransomware* son:

- Embargos judiciales.
- Reportes a centrales de riesgo.
- Alarmas de transferencias no consentidas.
- Foto comparendo.
- Citaciones judiciales.

Los principales vectores de un ataque DDos son:

- Reconocimiento y escaneo de los servicios de la compañía a afectar.
- Utilización de redes *Botnet* para lanzar ataques dirigidos a los servicios *online*.
- Interrupción de los servicios para los usuarios y terceros (clientes).
- Exigencia mediante correo electrónico o chat de ciber extorsión.
- Solicitud y demanda de pagos en criptomonedas, principalmente Bitcoins.

Los principales vectores de un ataque *malware* son:

- Correos con notificación de suplantación de identidad.
- Redirección hacia sitios web infectados.
- Descarga de aplicaciones maliciosas.[7]

[7] CCIT.ORG. Informe de las tendencias del cibercrimen en Colombia (2019-2020). [Sitio web]. Colombia:[Consulta: 23 de marzo 2020]. Disponible en https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Con las noticias y estadísticas anteriores se puede identificar la importancia de adoptar una metodología que permita identificar las vulnerabilidades existentes en los sistemas informáticos de los hospitales y como prevenirlos, porque sin importar el escenario de un ciberataque y el impacto que tenga para la organización, esta debe estar preparada para gestionarlo y mitigarlo.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo una metodología de pruebas de penetración e intrusión puede ayudar a prevenir ataques cibernéticos y bajar las estadísticas de ellos en el sector salud?

2. JUSTIFICACIÓN

La seguridad e integridad de la información se ha vuelto un factor crítico para todas las entidades, en especial las del sector salud, debido a que este tipo de entidades en los últimos años han estado en el ojo del huracán por el aumento de la cantidad de ataques cibernéticos y el robo de información sensible que se ha tenido, por lo tanto es importante brindar un servicio confiable y seguro a los pacientes y EPS asociadas, en donde se garantice la confidencialidad, integridad y disponibilidad de los datos.

Actualmente la Clínica no cuenta con una metodología para auditar la seguridad en los dispositivos de red que hacen parte de la historia clínica electrónica y que contiene datos sensibles de sus pacientes, por esta razón, surge de la necesidad de aplicar la metodología PTES y garantizar un sistema seguro, donde sea confiable la transmisión y almacenamiento de la información.

La ejecución de la metodología PTES, consta de siete fases para realizar pruebas de penetración efectiva, entorno a la seguridad actual de los dispositivos que conforman la red, con el objetivo de garantizar una infraestructura tecnológica que se adapte a las necesidades de la Clínica, que ayude a minimizar los riesgos, y cumpla con los lineamientos de seguridad exigidos.

Implementar acciones de mejora para mitigar los riesgos y mejorar la seguridad en el procesamiento de información sensible, trae consigo beneficios y valores agregados de forma directa e indirecta, que ayudaran en la administración, estabilidad, seguridad, escalabilidad y control de las plataformas tecnológicas, en donde se puede reflejar en el apalancamiento de nuevos negocios con EPS y pacientes satisfechos que se sienten respaldados por una entidad que protege sus datos.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Identificar las vulnerabilidades existentes en los dispositivos de red que hacen parte de la historia clínica electrónica de la Clínica Medellín, basado en la metodología PTES.

3.2. OBJETIVOS ESPECÍFICOS

- Establecer las vías de ataque disponibles para la aplicación de historia clínica electrónica según los planes de contingencia, equipo técnico, infraestructura de red y seguridad de la Clínica Medellín.

- Generar un análisis de vulnerabilidades existentes en la aplicación de historia clínica electrónica a través de una herramienta de seguridad informática.

- Clasificar las vulnerabilidades encontradas en la aplicación de historia clínica electrónica, con relación a su nivel de criticidad.

- Describir las vulnerabilidades que impactan de manera negativa a la clínica.

4. MARCO REFERENCIAL

3.1 MARCO TEÓRICO

Con el avance de la tecnología y el aumento de ataques a las vulnerabilidades de los sistemas informáticos, es necesario implementar metodologías de seguridad y herramientas que protejan y fortalezcan los sistemas que procesan o almacenen información sensible. Es importante conocer que se protege, que lo puede afectar y como se puede defender, antes de iniciar o implementar alguna estrategia.

3.1.1 Vulnerabilidades. Una vulnerabilidad, es una debilidad presente en un sistema operativo, software o sistema que le permite a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones. Las vulnerabilidades se pueden clasificar por su nivel de impacto de la siguiente manera:

- **Nivel de impacto Crítico:** La vulnerabilidad permite que la amenaza se propague sin que el usuario realice acciones.
- **Nivel de impacto Alto:** Coloca en riesgo la confidencialidad, integridad o disponibilidad de la información o de los recursos de procesamiento.
- **Nivel de impacto Medio:** No afecta a muchos usuarios y se puede combatir fácilmente con configuraciones, auditorias, entre otros.
- **Nivel de impacto Bajo:** Su impacto es mínimo y es difícil que un atacante la pueda aprovechar.

Se pueden encontrar diferentes tipos de vulnerabilidades:

- **Vulnerabilidades de desbordamiento de buffer:** Cuando una aplicación no es capaz de controlar la cantidad de datos que se copian en buffer. Este problema se puede aprovechar para ejecutar código que otorga a un atacante privilegios de administrador.

- **Vulnerabilidades de error de formato de cadena:** Es la condición de aceptar sin validar la entrada de datos proporcionada por el usuario. Este es un error de diseño de la aplicación.

- **Vulnerabilidades de inyección SQL:** Se producen cuando mediante alguna técnica se inserta o adjunta código SQL que no formaba parte de un código SQL programado.

- **Vulnerabilidades de denegación del servicio:** Excesivo consumo del ancho de banda de la red o de los recursos conectados al sistema informático, por medio de muchas peticiones por el atacante, evitando que los usuarios no puedan utilizar un servicio, aplicación o recurso.[8]

- Las vulnerabilidades más peligrosas son aquellas que le permiten a un atacante ejecutar código arbitrario, lo que le brindaría la oportunidad de tomar el control de la computadora y someterla a sus deseos o requerimientos. Estas vulnerabilidades, también conocidas por muchos usuarios como “agujeros de seguridad”, son una fuente prácticamente inagotable de problemas y por esto es recomendable mantener todos los sistemas actualizados, implementar firewall y WAF de aplicación, antivirus actualizado, conciencia en las personas que interactúan en el sistema y las aplicaciones y realizar auditorías periódicas que nos permitan asegurar todo el sistema informático.

3.1.2 Metodologías de pruebas de penetración. Para auditar los procesos y mantener los sistemas informáticos y aplicaciones seguros, existen varias metodologías que otorgan los controles necesarios para estar protegidos y minimizar las brechas de seguridad y vulnerabilidades, aquí la descripción de algunas de ellas:

4.1.2.1 Metodología OWASP. Consta de dos fases que son modo pasivo y modo activo, en el modo pasivo evalúa el sistema con diferentes herramientas buscando comprender la lógica de la aplicación. En el modo activo realiza diferentes pruebas por todo el sistema dividiendo las pruebas en diferentes categorías.[9]

- **Categoría de recopilación de información:** Se realizan pruebas de firma digital de la aplicación web, técnicas de *spidering* y *googling*, análisis de configuración

[8] TECNOLOGIA + INFORMATICA. Tipos de vulnerabilidades en informática. [Sitio web]. Colombia: [Consulta: 30 de marzo 2020]. Disponible en https://www.tecnologia-informatica.com/vulnerabilidades-informaticas/

[9] Reyes, Alonso. Metodología de Pruebas OWASP. [Sitio web]. Colombia: [Consulta: 30 de marzo 2020]. Disponible en http://www.reydes.com/d/?q=Metodologia_de_Pruebas_OWASP

del sistema, prueba de manejo de extensión de archivos, análisis de códigos de errores y también se verifican los archivos antiguos y las copias de seguridad.

- **Categoría de Autentificación:** Se realizan pruebas con diccionarios sobre cuentas de usuario para intentar saltarse la autentificación, atravesar directorios y acceder a archivos, sistemas de recordatorios y *reset* de *password* vulnerables.

- **Categoría de gestión de sesiones:** Se analizan las variables de sesión expuesta mediante varios métodos y aplicando varias inyecciones de código.

- **Categoría de validación de datos**: Se realiza un análisis mediante la inserción de comandos del sistema operativo, se realizan pruebas de desbordamiento de Búfer y también se revisa el bloqueo de cuentas de usuario.

- **Categoría de pruebas de denegación de servicio:** Se profundiza más en el análisis de desbordamiento de Búfer se realizan pruebas de uso de entradas de usuario como bucle y pruebas de almacenamiento excesivo en una sesión.

- **Categoría de comprobación de servicios web:** Se analizan las pruebas estructurales de XML, pruebas de repetición, parámetros HTTP y XML a niveles de contenido y por último se revisan los adjuntos SOAP maliciosos que son protocolos estándares para definir la comunicación entre dos objetos mediante el intercambio de datos XML.

- **Categoría de pruebas AJAX:** Las aplicaciones Ajax se extienden entre el cliente y el servidor, por ende, tienen mayor superficie para ser atacadas por lo que en esta parte, se realizan pruebas de la mayor cantidad de técnicas de ataques que existen por ser tan delicadas.

4.1.2.2 Metodología PTES. Es una metodología muy completa que cubre la técnica, así como otros aspectos importantes de una prueba de penetración, como la afluencia del alcance, informando y protegiendo la información y el endurecimiento de sus sistemas físicos y virtuales.[10]

[10] BLOGSPOT. Metodología PTES (Penetration Testing Execution Standard). [Sitio web]. Colombia: [Consulta: 30 de marzo 2020]. Disponible en http://blogdeauditoriadeseguridad.blogspot.com/2017/09/metodologia-ptes-penetration-testing.html

Consiste en siete fases de pruebas de penetración efectiva en el entorno de la empresa, las fases son:

- **Interacciones previas:** Definir los puntos y la profundidad a evaluar, las fechas de la evaluación, los tiempos estimados, entre otros aspectos relevantes. En esta fase se deja claro el alcance y el objetivo general, los dispositivos de red que se analizarán y los tiempos estimados de ejecución. La metodología PTES cuenta con un cuestionario para comprender la misión, visión y demás información acerca de la empresa.

- **Recolección de Información:** Obtener y recopilar toda la información posible sobre la empresa y el objetivo, esta recolección se divide en 3 tipos, el primero es la recolección de información simple por medio de herramientas. El segundo es la recolección de información con un análisis más profundo por medio del conocimiento de los procesos y estructura de la empresa. El tercero es la recolección de información avanzada por medio del conocimiento a profundidad de todo lo relacionado con la empresa. Esta fase es muy importante para determinar los posibles ataques y atacantes.

- **Modelado de amenaza:** Para esta fase no se tiene definido un estándar, pero se debe analizar los planes de contingencia, así como el equipo técnico, las instalaciones (redes, *hardware* y *software*), las herramientas disponibles para analizar la efectividad de las diversas vías de ataque disponibles y las amenazas. Para esta fase se debe tener en cuenta el impacto que genera cada uno de los escenarios donde pueda ser explotada una vulnerabilidad existente. Esta fase es importante porque se priorizan los activos para llevar a cabo los procedimientos y posteriores controles.

- **Análisis de vulnerabilidades:** Con los datos recogidos en la fase anterior, se detectan las vulnerabilidades existentes y se buscan las posibles vías y métodos de ataque, así como información sobre usuarios, nombres de equipos, métodos de ataque, entre otros. Para esta fase se debe establecer el alcance de la amplitud y profundidad de la prueba de *pentesting*. Cuando termine esta fase se listan los objetivos que pueden ser atacados en la fase siguiente.

- **Explotación:** Se configuran las herramientas de *pentesting* con el objetivo de atacar a las vulnerabilidades detectadas para comprometer el sistema y obtener acceso por medio de las brechas de seguridad existentes. Para esta fase se debe tener conocimiento de los dispositivos de red o software que tiene la

empresa para contrarrestar el ataque y personalizar los ataques para explotar las vulnerabilidades exitosamente.

- **Post-Explotación:** Se persiste en obtener acceso al sistema de manera perdurable en el tiempo de manera que se pueda realizar en un tiempo indeterminado el ataque a las vulnerabilidades detectadas. En esta fase se analiza el valor del dispositivo comprometido con la prueba con base a la información que almacena, los privilegios de acceso a otros dispositivos para ingresar a la red. En esta fase se deben asignar los roles para proteger la información y las responsabilidades, se debe realizar la configuración del *exploit* con el objetivo de ingresar a la red sin colocarla en riesgo.

- **Informe final:** La metodología no cuenta con un formato específico para el informe final de las pruebas de *pentesting*, pero si presenta los aspectos para tener en cuenta en él. En este informa se debe documentar el contexto de las pruebas, los lineamientos y objetivos que se alcanzaron, listar las vulnerabilidades de acuerdo con su nivel de criticidad, los riesgos encontrados y realizar recomendaciones para mitigarlos.

La metodología PTES surge con la evolución y el avance de los sistemas informáticos con el objetivo de establecer los procesos de auditoria a los sistemas de información. PTES se estructuró para guiar detalladamente un proceso de *pentesting* comenzando con la recolección de la información hasta el informe de las vulnerabilidades encontradas. La prueba de *pentesting* debe determinar todo lo relacionado con el ataque hasta llegar al objetivo para detallar las brechas de seguridad.

4.1.2.3 Metodología OSSTMM. Esta metodología comprende seis secciones para proteger e implementar medidas de seguridad sobre los sistemas informáticos, otorgando los controles necesarios para mitigar las vulnerabilidades existentes, a continuación, se nombran cada una de las fases:

- **Seguridad de la Información:** Revisión de la inteligencia competitiva, la revisión de la privacidad y la recolección de documentos en un ámbito de seguridad de los datos.

- **Seguridad de los Procesos:** Testeo de solicitud, de sugerencia dirigida y testeo de las personas confiables.

- **Seguridad en las Tecnologías de Internet:** Logística y controles, sondeo de red igualmente, la identificación de los servicios de sistemas.

- **Seguridad en las Comunicaciones:** Testeo de PBX, correo de voz, fax y *modems*.

- **Seguridad Inalámbrica:** Verificación de: Radiación Electromagnética (EMR), Redes Inalámbricas [802.11], Redes Bluetooth, Dispositivos de Entrada Inalámbricos, Dispositivos de Mano Inalámbricos, Comunicaciones sin Cable.

- **Seguridad Física:** Revisión de perímetro, monitoreo, respuesta de alarmas, ubicación y entorno. Igualmente, la evaluación de controles de acceso.[11]

4.1.2.4 Metodología ISSAF. Realiza un análisis detallado de todos los posibles aspectos que afectan al testeo de seguridad. La información contenida dentro de ISSAF, se encuentra organizada alrededor de lo que se ha dado en llamar "criterios de evaluación", cada uno de los cuales ha sido escrito y revisado por expertos en cada una de las áreas de aplicación.[12]

Estos criterios de evaluación a su vez se componen de los siguientes ítems:

- Una descripción del criterio de evaluación.
- Puntos y objetivos para cubrir.
- Los prerrequisitos para conducir la evaluación.
- El proceso mismo de evaluación.
- El informe de los resultados esperados.
- Las contramedidas y recomendaciones.
- Referencias y Documentación Externa.

Para organizar de forma sistemática las labores de testeo, dichos "Criterios de Evaluación", se han catalogado, desde los aspectos más generales, como pueden

[11] GLOBATIKA LAB. Metodología OSSTMM. [Sitio web]. Colombia:[Consulta: 30 de marzo 2020]. Disponible en https://peritosinformaticos.es/metodologia-osstmm/

[12] INSECUREDATA. Metodología de test de intrusión ISSAF. [Sitio web]. Colombia:[Consulta: 30 de marzo 2020]. Disponible en http://insecuredata.blogspot.com/2009/04/metodologia-de-test-de-intrusion-issaf.html#:~:text=La%20metodolog%C3%ADa%20de%20test%20de,Planificaci%C3%B3n%20y%20Preparaci%C3%B3n

ser los conceptos básicos de la “Administración de Proyectos de Testeo de Seguridad”, hasta técnicas tan puntuales como la ejecución de pruebas de Inyección de Código SQL o como las “Estrategias del *Cracking* de Contraseñas.[13]

4.1.3 Herramientas de *pentesting.* Para analizar las vulnerabilidades de los sistemas informáticos y aplicaciones, existen varias herramientas de pentesting que permiten hallar vulnerabilidades en los sistemas informáticos e intentar explotarlas, a continuación, se describen algunas de ellas:

4.1.3.1 Herramienta Maltego. Permite recoger información en internet y cruzar información para obtener acceso a servidores de correo y redes sociales de personas o empresas. Funciona de la siguiente manera: Maltego envía la petición a los servidores de semillas en formato XML a través de HTTPS. La petición del servidor de la semilla se da a los servidores TAS que se transmiten a los proveedores de servicios.[14]

4.1.3.2 Herramienta NESSUS. Es un programa de escaneo de vulnerabilidades en diversos sistemas operativos e informa sobre su estado, consiste en realizar un escaneo ya sea programado o manual, en el sistema que se selecciona, se debe busca puertos abiertos con NMAP e intenta atacarlos con exploits. Algunas pruebas realizadas con NESSUS pueden generar caída en los sistemas, por esto se debe desactivar la opción de pruebas no seguras antes del escaneo. Al final realiza un reporte de los resultados que se puede descargar donde permite ver el CVE- ID asociado, detalle y recomendación de mitigación de las vulnerabilidades encontradas.[15]

4.1.3.3 Herramienta NMAP. Descubre redes y el estado de sus puertos TCP y UDP e identifica la versión del sistema operativo. Cuenta con la funcionalidad NSE, que permite la ejecución de scripts para automatizar tareas como escaneo y explotación de vulnerabilidades, auditorias de seguridad, detección de malware, entre otras.[16]

---

[13] MEDIUM. ¿Qué es el pentesting?. [Sitio web]. Colombia:[Consulta: 30 de marzo 2020]. Disponible en https://medium.com/@rootsec/pentesting-introducci%C3%B3n-cb40a8ae67ba

[14] Perez, Ivan. Maltego, la herramienta que te muestra qué tan expuesto estás en Internet. [Sitio web]. Colombia:[Consulta: 30 de marzo 2020]. Disponible en https://www.welivesecurity.com/la-es/2014/02/19/maltego-herramienta-muestra-tan-expuesto-estas-internet/

[15] Catoira, Fabio. Funcionalidades de monitoreo continuo de Nessus. [Sitio web]. Colombia: [Consulta: 30 de marzo 2020]. Disponible en www.welivesecurity.com/la-es/2017/10/27/reglas-de-yara-nessus

[16] Lagos, Edwin. Análisis de vulnerabilidades y pruebas de penetración a la infraestructura tecnológica de empresa. [Sitio web]. Colombia: [Consulta: 30 de marzo 2020]. Disponible en

4.1.3.4 Herramienta WIRESHARK. Es un analizador que permite capturar y explorar, de forma interactiva, el tráfico presente en una red, sus características incluyen la captura en tiempo real y el análisis *offline*, y una inspección profunda de cientos de protocolos. permite ver, aun nivel bajo y detallado, consultar todo lo que está ocurriendo en la red.[17]

A continuación, se realiza un cuadro comparativo de las herramientas de *pentesting* mencionadas anteriormente:

Cuadro 2. Comparativo de las herramientas de *pentesting*

Herramienta	Función principal	Características	Tipo de licencia
Maltego	Recolecta información en internet para obtener acceso a servidores empresas o redes sociales.	Es de uso fácil e intuitivo, flexible en los métodos de búsqueda y permite diferentes tipos de vista de los resultados.	Libre de Código Abierto
Nessus	Busca puertos abiertos con NMAP e intenta vulnerarlos con *exploits*.	Multiplataforma, permite ver un informe detallado con el CVE- ID asociado, detalle y recomendación de mitigación de las vulnerabilidades encontradas.	La versión home es libre y la versión *work* es paga y sin restricciones
Nmap	Descubre redes y el estado de sus puertos TCP y UDP y permite la ejecución de scripts para automatizar tareas.	Flexible, multiplataforma, está basado en comandos, se encuentra bien documentado ya que es una herramienta muy popular.	Libre de Código Abierto
Wireshark	Permite ver, aun nivel bajo y detallado, consultar todo lo que está ocurriendo en la red	Multiplataforma, soporta múltiples protocolos, reconstruye sesiones TCP y su interfaz gráfica es de fácil manejo.	Libre de Código Abierto

Fuente Propia

http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/15381/Informe.pdf?sequence=1

[17] Lagos, Edwin. Wireshark. [Sitio web]. Colombia: [Consulta: 30 de marzo 2020]. Disponible en https://www.ecured.cu/Wireshark

Las herramientas de *pentesting* que se compararon en la tabla anterior ayuda a tener un acercamiento a sus característica y funcionalidades, con lo cual, se puede elegir la mejor opción, teniendo en cuenta el tipo de licenciamiento.

5. MARCO CONCEPTUAL

Desde siempre las empresas tienen la tarea de asegurar los datos sensibles que almacenan, y gracias a la seguridad informática se mantiene la confidencialidad, integridad y disponibilidad de la información, implementando técnicas de protección como el despliegue de las tecnologías antivirus, *firewalls*, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes que establecen la forma de actuar y asegurar las situaciones de amenazas, vulnerabilidades o fallas parciales o totales.

Los avances tecnológicos y digitales han obligado a adaptar leyes que permitan controlar los procesos que se realizan a través de medios informáticos y brindar herramientas que ayuden a reducir los posibles riesgos de infraestructura, sistemas operativos, bases de datos que interactúan en el procesamiento de la información.

En Colombia, se han establecido leyes que establecen normativas sobre las transacciones electrónicas y la seguridad de la información a través de:

La Ley No. 1273 del 2009 (Delitos Informáticos): que penaliza todos los actos criminales sobre los sistemas de información, como, por ejemplo: accesos no autorizado a sistemas informáticos, uso y venta de *software* malicioso, violación de datos informáticos, suplantación de sitios web para capturar datos personales, hurto por medios informáticos, entre otros.[18]

A nivel internacional normas como ISO/IEC27001:2013, que define los requisitos para implementar, establecer y mantener un SGSI (Sistema de Gestión de Seguridad de la Información), cuenta con tiene 14 dominios, 35 objetivos de control y 114 controles relacionados con las políticas de seguridad, aspectos organizativos de la seguridad de la información, control de accesos, seguridad de las telecomunicaciones, adquisición, desarrollo y mantenimiento de los sistemas de información, gestión de incidentes en la seguridad de la información, entre otros.[19]

[18] MINTIC. Ley 1273 de 2009. [Sitio web]. Colombia:[Consulta: 10 de abril 2020]. Disponible en https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

[19] ISO. ISO 27002:2013. [Sitio web]. Colombia:[Consulta: 10 de abril 2020]. Disponible en https://www.efectus.cl/wp-content/uploads/2018/12/Controles_ISO27002-2013.pdf

Estas normas son esenciales para especificar y forzar el cumplimiento de políticas que son establecidas para, gestionar y controlar de una manera más eficiente, los recursos y activos de información.

Dada a la importancia y el valor que posee la información en todos sus aspectos, los modelos, estándares, buenas prácticas y metodología de intrusión como PTES, que cubre la técnica, así como otros aspectos importantes de una prueba de penetración, como la fluencia del alcance, informando y protegiendo la información y el endurecimiento de sus sistemas físicos y virtuales, son elecciones oportunas para proteger el activo de información más valioso que tiene una compañía.[20]

Por lo anterior, su elección se realiza sin obligatoriedad, sin embargo, la necesidad de proteger un elemento que fácilmente no es sustituible por otras vicisitudes exige, que estos lineamientos de seguridad sean considerados de manera imperativa para una empresa, donde se considere un análisis sobre los riesgos informáticos más recurrentes que haya tenido la organización en contraste, con las amenazas a las que se encuentre expuesta.

5.1. MARCO HISTÓRICO

5.1.1. **Metodología PTES.** Es una metodología muy completa que cubre la técnica, así como otros aspectos importantes de una prueba de penetración, como la fluencia del alcance, informando y protegiendo la información y el endurecimiento de sus sistemas físicos y virtuales.[21]

Consiste en siete fases de pruebas de penetración efectiva en el entorno de la empresa, las fases son:

- **Interacciones previas:** Definir los puntos y la profundidad a evaluar, las fechas de la evaluación, los tiempos estimados, entre otros aspectos relevantes. En esta fase se deja claro el alcance y el objetivo general, los dispositivos de red que se analizaran y los tiempos estimados de ejecución. La metodología PTES

[20] BLOGSPOT. Metodología PTES (Penetration Testing Execution Standard). [Sitio web]. Colombia:[Consulta: 30 de marzo 2020]. Disponible en http://blogdeauditoriadeseguridad.blogspot.com/2017/09/metodologia-ptes-penetration-testing.html

[21] BLOGSPOT. Metodología PTES (Penetration Testing Execution Standard). [Sitio web]. Colombia:[Consulta: 30 de marzo 2020]. Disponible en http://blogdeauditoriadeseguridad.blogspot.com/2017/09/metodologia-ptes-penetration-testing.html

cuenta con un cuestionario para comprender la misión, visión y demás información acerca de la empresa.

- **Recolección de Información:** Obtener y recopilar toda la información posible sobre la empresa y el objetivo, esta recolección se divide en 3 tipos, el primero es la recolección de información simple por medio de herramientas. El segundo es la recolección de información con un análisis más profundo por medio del conocimiento de los procesos y estructura de la empresa. El tercero es la recolección de información avanzada por medio del conocimiento a profundidad de todo lo relacionado con la empresa. Esta fase es muy importante para determinar los posibles ataques y atacantes.

- **Modelado de amenaza:** Para esta fase no se tiene definido un estándar, pero se debe analizar los planes de contingencia, así como el equipo técnico, las instalaciones (redes, hardware y software), las herramientas disponibles para analizar la efectividad de las diversas vías de ataque disponibles y las amenazas. Para esta fase se debe tener en cuenta el impacto que genera cada uno de los escenarios donde pueda ser explotada una vulnerabilidad existente. Esta fase es importante porque se priorizan los activos para llevar a cabo los procedimientos y posteriores controles.

- **Análisis de vulnerabilidades:** Con los datos recogidos en la fase anterior, se detectan las vulnerabilidades existentes y se buscan las posibles vías y métodos de ataque, así como información sobre usuarios, nombres de equipos, métodos de ataque, entre otros. Para esta fase se debe establecer el alcance de la amplitud y profundidad de la prueba de *pentesting*. Cuando termine esta fase se listan los objetivos que pueden ser atacados en la fase siguiente.

- **Explotación:** Se configuran las herramientas de *pentesting* con el objetivo de atacar a las vulnerabilidades detectadas para comprometer el sistema y obtener acceso por medio de las brechas de seguridad existentes. Para esta fase se debe tener conocimiento de los dispositivos de red o software que tiene la empresa para contrarrestar el ataque y personalizar los ataques para explotar las vulnerabilidades exitosamente.

- **Post-Explotación:** Se persiste en obtener acceso al sistema de manera perdurable en el tiempo de manera que se pueda realizar en un tiempo indeterminado el ataque a las vulnerabilidades detectadas. En esta fase se analiza el valor del dispositivo comprometido con la prueba con base a la

información que almacena, los privilegios de acceso a otros dispositivos para ingresar a la red. En esta fase se deben asignar los roles para proteger la información y las responsabilidades, se debe realizar la configuración del *exploit* con el objetivo de ingresar a la red sin colocarla en riesgo.

- **Informe final:** La metodología no cuenta con un formato específico para el informe final de las pruebas de *pentesting*, pero si presenta los aspectos a tener en cuenta en él. En este informa se debe informar el contexto de las pruebas, los lineamientos y objetivos que se alcanzaron, listar las vulnerabilidades de acuerdo con su nivel de criticidad, los riesgos encontrados y realizar recomendaciones para mitigarlos.

La metodología PTES surge con la evolución y el avance de los sistemas informáticos con el objetivo de establecer los procesos de auditoria a los sistemas de información. PTES se estructuró para guiar detalladamente un proceso de *pentesting* comenzando con la recolección de la información hasta el informe de las vulnerabilidades encontradas. La prueba de *pentesting* debe determinar todo lo relacionado con el ataque hasta llegar al objetivo para detallar las brechas de seguridad.

La metodología no ha sido actualizada y se conserva en su versión 1, se tiene pensado una versión 2, donde se especificarán a gran detalle los niveles, pero si es muy detallista en cuanto a su objetivo y tiene niveles de detalle altos y definidos que hacen que la implementación sea muy sencilla y se pueda aplicar en cualquier sistema, arquitectura o aplicativo. PTES ha sido adoptada por varios profesionales y es un gran referente en los libros de *pentesting* como, por ejemplo, *Metasploit*.[22]

5.2. ANTECEDENTES O ESTADO ACTUAL

La Clínica, ha implementado buenas prácticas con base a la norma NTC-ISO-IEC 27001:2013:

[22] MEDIUM. Pentesting. [Sitio web]. Colombia:[Consulta: 30 de marzo 2020]. Disponible en https://medium.com/@rootsec/pentesting-introducci%C3%B3n-cb40a8ae67ba

5.2.1. Almacenamiento de las bases de datos. La clínica debe informar a los pacientes que las bases de datos de la clínica se almacenan automatizadamente en computadores y/o servidores propios de la empresa. Igualmente existen algunas bases de datos que se almacenan físicamente.

5.2.2. Inscripción en el registro de bases de datos de la superintendencia de industria y comercio. La clínica debe acatar y cumplir las obligaciones que la normatividad le imponga en relación con el registro e informes que deba entregar a las autoridades competentes. Para efectos del registro de las bases de datos, la Clínica debe realizar un inventario teniendo en cuenta los siguientes parámetros:

- Cantidad de bases de datos con información personal.
- Cantidad de pacientes por cada base de datos.
- Información detallada de los canales o medios que se tienen previstos para atender a los pacientes.
- Tipo de datos personales contenidos en cada base de datos a los que se realiza tratamiento, como: datos de identificación, ubicación, socioeconómicos, sensibles u otros.
- Ubicación física de las bases de datos, al respecto se preguntará si la base de datos se encuentra almacenada en medios propios, por ejemplo, archivadores o servidores (dependiendo de si se trata de un archivo físico o una base de datos electrónica), internos o externos a las instalaciones físicas del responsable.
- Cuando el tratamiento de los datos personales se realice a través de un (unos) encargado (s), se solicitarán los datos de identificación y ubicación de ese (esos) encargado (s).
- Medidas de seguridad y/o controles implementados en la base de datos para minimizar los riesgos de un uso no adecuado de los datos personales tratados.
- Información sobre si se cuenta con la autorización de los pacientes de los datos contenidos en las bases de datos.
- Forma de obtención de los datos (directamente del paciente o mediante terceros).
- Cuando se ha realizado transferencia o transmisión internacional de la base de datos, se solicitará la información básica del destinatario.
- Si la base de datos se ha cedido, se solicitará la información básica del cesionario.

5.2.3. Derechos del paciente sobre los datos. De acuerdo con lo contemplado por la normatividad vigente aplicable en materia de protección de datos, los siguientes son los derechos de los titulares de los datos personales:

- Acceder, conocer, actualizar y rectificar sus datos personales frente a la Clínica en su condición de responsable del tratamiento. Este derecho se podrá ejercer, entre otros, frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
- Solicitar prueba de la autorización otorgada a la Clínica para el tratamiento de datos, mediante cualquier medio válido, salvo en los casos en que no es necesaria la autorización.

5.2.4. Responsable del tratamiento. La Clínica esta presentada legalmente por el gerente, quien es el responsable del tratamiento de los datos personales y las bases de datos.

5.2.5. Encargado del tratamiento. Los encargados del tratamiento de datos personales bajo el compromiso de la clínica es el coordinador de cada una de las áreas y dependencias administrativas de la que provenga institucionalmente la solicitud de tratamiento de datos.

Todos los trabajadores de la Clínica deben aceptar la política y las instrucciones y procedimientos que se impartan para su adecuado cumplimiento. Se exige al personal vinculado el conocimiento de los deberes que deben cumplir.

5.2.6. Evaluación y revisión continua por parte del encargado del tratamiento de datos personales. El Encargado del tratamiento de datos personales de la Clínica, como protector y garante de los derechos de los titulares y custodio de los datos suministrados frente a su leal y correcto tratamiento, llevará a cabo las siguientes acciones de evaluación y revisión:

- Controlar y actualizar el inventario de información personal continuamente para identificar y evaluar nuevas recolecciones, usos y divulgaciones.
- Revisar las políticas siguiendo los resultados de las evaluaciones o auditorías.

- Mantener como documentos históricos las evaluaciones de impacto y las de amenazas a la seguridad y riesgos.
- Revisar y actualizar, en forma periódica, la formación y la educación impartida a todos los empleados de la organización, como resultado de evaluaciones continuas y comunicar los cambios realizados a los controles del programa.

5.2.7. Confidencialidad y seguridad de las bases de datos. La Clínica debe aplicar las mejores prácticas para la seguridad, discreción y confidencialidad de los datos personales de los pacientes. Debe verificar cuando corresponda, la procedencia de las excepciones legales para entregar los datos personales a las autoridades en los casos pertinentes.

Los datos de naturaleza reservada podrán ser proporcionados de manera escrita, oral, por medios electrónicos, magnéticos o digitales, o bien, por virtud de revisión de libros, expedientes o documentos.

La protección de la información de naturaleza reservada, confidencial o privilegiada a cargo de la Clínica se debe desarrollar mediante los protocolos de seguridad de la información y los acuerdos marcos de confidencialidad establecidos para proteger la información, por lo que su divulgación o revelación estará estrictamente supeditada a las estipulaciones establecidas en los instrumentos legales. En consecuencia, de lo anterior, es un deber de la Clínica velar por el cumplimiento de las estipulaciones confidenciales y reservadas frente a terceros y por lo tanto debe guardar absoluta reserva sobre los datos que deban ser protegidos por estas disposiciones. En ninguna circunstancia se revelarán datos que hagan parte de un secreto industrial o comercial.

5.2.8. Seguridad de la información. La Clínica debe contar con distintas medidas de seguridad de la información dentro de las cuales se encuentran las siguientes:

- Política de seguridad de la información.
- Manual de procedimiento de contingencias de la información.
- Acuerdos marco de confidencialidad suscrito por los empleados de la clínica.
- Medidas de seguridad especiales para almacenamiento de bases de datos con datos sensibles.

5.2.9. Autorización y consentimiento del paciente. La Clínica requiere del consentimiento libre, previo, expreso e informado del titular de los datos personales para el tratamiento de estos, exceptos en los casos expresamente autorizados en la ley:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones
- legales o por orden judicial.
- Datos de naturaleza pública.
- Tratamiento de información autorizado por la ley para fines históricos o estadísticos.
- Datos relacionados con el Registro Civil de las Personas.

5.3. MARCO LEGAL

El conjunto de normas que regula el tratamiento de datos personales en la Clínica es el siguiente:

5.3.1. Constitución Política, artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley. Con el fin de prevenir la comisión de actos terroristas, una ley estatutaria reglamentará la forma y condiciones en que las autoridades que ella señale, con fundamento en serios motivos, puedan interceptar o registrar la correspondencia y demás formas de comunicación privada, sin previa orden judicial, con aviso inmediato a la Procuraduría General de la Nación y control judicial posterior dentro de las treinta y seis (36) horas siguientes. Al iniciar cada período de sesiones el Gobierno rendirá informe al Congreso sobre el uso que se haya hecho de esta facultad. Los funcionarios que abusen de las medidas a que se refiere

este artículo incurrirán en falta gravísima, sin perjuicio de las demás responsabilidades a que hubiere lugar.[23]

5.3.2. Ley 1266 de 2008. La presente ley se aplica a todos los datos de información personal registrados en un banco de datos, sean estos administrados por entidades de naturaleza pública o privada.

Esta ley se aplicará sin perjuicio de normas especiales que disponen la confidencialidad o reserva de ciertos datos o información registrada en bancos de datos de naturaleza pública, para fines estadísticos, de investigación o sanción de delitos o para garantizar el orden público.

Se exceptúan de esta ley las bases de datos que tienen por finalidad producir la Inteligencia de Estado por parte del Departamento Administrativo de Seguridad, DAS, y de la Fuerza Pública para garantizar la seguridad nacional interna y externa.

Los registros públicos a cargo de las cámaras de comercio se regirán exclusivamente por las normas y principios consagrados en las normas especiales que las regulan.

Igualmente, quedan excluidos de la aplicación de la presente ley aquellos datos mantenidos en un ámbito exclusivamente personal o doméstico y aquellos que circulan internamente, esto es, que no se suministran a otras personas jurídicas o naturales.[24]

5.3.3. Ley 1581 de 2012. La presente ley se aplica al tratamiento de datos personales efectuado en territorio colombiano o cuando al responsable del tratamiento o encargado del tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.

[23] CONSTITUCIÓN POLITICA DE COLOMBIA. Artículo 15. [Sitio web]. Colombia:[Consulta: 20 de abril 2020]. Disponible en https://www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-15#:~:text=fundamentales%20%2F%20Art%C3%ADculo%2015-,Art%C3%ADculo%2015,debe%20respetarlos%20y%20hacerlos%20respetar

[24] FUNCIÓN PUBLICA. Ley 1266 de 2008. [Sitio web]. Colombia: [Consulta: 20 de abril 2020]. Disponible en https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

El régimen de protección de datos personales que se establece en la presente ley no será de aplicación:

- A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.

- Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al titular y solicitar su autorización. En este caso los responsables y encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley;

- A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo.

- A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia.

- A las bases de datos y archivos de información periodística y otros contenidos editoriales.

Parágrafo. Los principios sobre protección de datos serán aplicables a todas las bases de datos, incluidas las exceptuadas en el presente artículo, con los límites dispuestos en la presente ley y sin reñir con los datos que tienen características de estar amparados por la reserva legal.[25]

5.3.4. Decretos Reglamentario 1727 de 2009. Artículo 1°. Requisitos mínimos de información. Para los efectos de lo consagrado en el artículo 14 de la Ley 1266 de 2008, los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, al presentar la información de los titulares deberán adoptar un formato que contenga, como mínimo, los datos requeridos en el presente decreto, según el sector al cual pertenezca la fuente de información.

[25] SUIN JURISCOL. Ley 1581 de 2012. [Sitio web]. Colombia:[Consulta: 20 de abril 2020]. Disponible en http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1684507

La información a la que se refiere el presente decreto deberá atender las características y particularidades de cada contrato celebrado.

- Nombre y apellidos completos o razón o denominación social: Deberá indicarse el nombre y apellidos o razón o denominación social del titular de la información, según se trate de persona natural o jurídica.

- Tipo y número de identificación: Deberá indicarse el tipo de documento y número de identificación del titular: Cédula de ciudadanía, cédula de extranjería, NIT.

- Fecha de corte de la información: Deberá indicarse la fecha a la cual corresponde la información que se reporta.

- Registro últimas consultas: Deberá indicarse el número de consultas realizadas en los últimos seis (6) meses.

- Fecha de la consulta: Deberá indicarse la fecha en la cual se lleva a cabo la consulta de la información.

Con fundamento en lo dispuesto en el artículo 14 de la Ley 1266 de 2008, en el encabezado de cada reporte de información deberá indicarse lo siguiente: "Se presenta reporte negativo cuando la(s) persona(s) naturales y jurídicas efectivamente se encuentran en mora en sus cuotas u obligaciones. Se presenta reporte positivo cuando la(s) persona(s) naturales y jurídicas están al día en sus obligaciones".[26]

5.3.5. Decretos Reglamentario 2952 de 2010. Incumplimiento de las obligaciones por fuerza mayor: En el evento en que el incumplimiento de la(s) obligación(es) dineraria(s) a cargo de un titular de información se origine en una situación de fuerza mayor causada por el secuestro, la desaparición o el desplazamiento forzados de dicho titular, este tendrá derecho a que el incumplimiento no se refleje como información negativa en su reporte.

El titular o las personas con las cuales tenga parentesco hasta el cuarto grado de consanguinidad, segundo de afinidad, primero civil, o con quien esté ligado por

[26] SUIN JURISCOL. Ley 1581 de 2012. [Sitio web]. Colombia:[Consulta: 20 de abril 2020]. Disponible en http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1684507

matrimonio o unión permanente, según sea el caso, podrán solicitar la actualización del reporte ante los operadores de información, observando el procedimiento previsto en el numeral II del artículo 16 de la Ley 1266 de 2008.

En el caso de que el titular se encuentre secuestrado, deberá allegarse al operador, la certificación judicial de la que trata el artículo 5° de la Ley 986 de 2005.

Si el titular ha sido desplazado forzosamente, deberá acreditarse ante el operador de la información, la inscripción en el Registro Único de Población Desplazada (RUPD), administrado por la Agencia Presidencial para la Acción Social y la Cooperación Internacional o la entidad que haga sus veces.

Las condiciones de víctima de secuestro, desaparición forzosa o la condición de desplazamiento forzado también podrán ser acreditadas por otros medios, tales como una certificación expedida por la Fiscalía General de la Nación, o quien haga sus veces, de la denuncia formalmente presentada del secuestro o de la desaparición forzada.

En todo caso, los documentos que se alleguen al operador deberán contener la identificación de la persona víctima del secuestro o desaparición forzada, nombres completos y documento de identidad, así como la fecha probable de ocurrencia del hecho.[27]

[27] SUIN JURISCOL. Ley 1581 de 2012. [Sitio web]. Colombia:[Consulta: 20 de abril 2020]. Disponible en http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1684507

6. DISEÑO METODOLÓGICO

Se adopta la Metodología PTES (Estándar para la ejecución de pruebas de penetración) y la herramienta de intrusión NESSUS, para escanear múltiples vulnerabilidades de diversos dispositivos informáticos, lo que permite a su vez cubrir la necesidad puntual del proyecto para encontrar las vulnerabilidades y realizar las recomendaciones pertinentes para fortalecer los dispositivos de red que hacen parte de la Historia Clínica Electrónica, contra las amenazas cibernéticas.

Para la recolección de la información se utilizara el método de análisis cualitativo que arroja datos de tipo descriptivo, porque se realizará el levantamiento de información por medio de algunas preguntas personalmente a algunas de las personas que interactúan en la Clínica y están directamente relacionadas con la aplicación de historia clínica electrónica y los dispositivos de red que hacen parte de ella, como lo son: Analista de historia clínica, Analista de infraestructura, Analista de servidores, Analista de base de datos y Auxiliar de soporte, para proceder con la interpretación de esa información recolectada y realizar el análisis y explotación de vulnerabilidades pertinentes.

Se generará un informe con los resultados obtenidos al aplicar la Metodología PTES, donde se relacionan las vulnerabilidades identificadas en los dispositivos de red que hacen parte de la Historia Clínica Electrónica en la Clínica y los posibles métodos de solución.

7. DESARROLLO DE LOS OBJETIVOS

7.1. DESARROLLO DE OBJETVO 1: ESTABLECER LAS VÍAS DE ATAQUE DISPONIBLES PARA LA APLICACIÓN DE HISTORIA CLÍNICA ELECTRÓNICA SEGÚN LOS PLANES DE CONTINGENCIA, EQUIPO TÉCNICO, INFRAESTRUCTURA DE RED Y SEGURIDAD DE LA CLÍNICA MEDELLÍN.

Para el desarrollo del objetivo 1 se utiliza la primera, segunda y tercera fase de la metodología PTES que consiste en obtener y recopilar toda la información posible sobre la empresa, definir los puntos y la profundidad a evaluar, los dispositivos de red que se analizarán, los tiempos estimados de ejecución, los planes de contingencia, el equipo técnico, las instalaciones (redes, hardware y software), las herramientas disponibles para analizar la efectividad de las diversas vías de ataque disponibles y las posibles amenazas existentes.

7.1.1 Integrantes del equipo de TI. El equipo de trabajo de TI de la Clínica está conformado por:

- **Jefe de sistemas:** Se encarga de diseñar y auditar las políticas o buenas prácticas de seguridad en los dispositivos que conforman la red, aplicaciones y bases de datos.

- **Analista de infraestructura:** Se encarga de la seguridad y administración de los dispositivos de red.

- **Analista de Servidores:** Se encarga de la seguridad y administración de los servidores.

- **Analista de historia clínica electrónica:** Se encarga de la administración de los módulos de historia clínica y protección de datos confidenciales.

- **Auxiliar de Sistemas:** Se encarga del soporte de los equipos clientes e instalación de aplicación de historia clínica.

7.1.2 Topología de red. La Clínica dentro de su infraestructura de red y seguridad cuenta con:

- **ISP:** Cuenta con dos canales de internet uno para los pacientes y visitantes y otro para la red corporativa. Adicional tienen un canal de datos dedicado para la conexión con otras sedes remotas.
- **Firewall:** Cuenta con dispositivos UTM en alta disponibilidad los cuales se encargan de proteger el perímetro de la red, servicios expuestos y red internet. Dentro de las funciones de este dispositivo se tiene:

    - Permitir y denegar tráfico entre VLANs
    - Permitir y denegar tráfico hacia internet
    - Exponer servicios a internet y otras redes externas a través de NATs
    - Asignación de DHCP para alguna VLANs
    - Tiene habilitado el módulo de IDS/IPS
    - Tiene habilitado el módulo de Antivirus
    - Presta el servicio de controladora para APs de la red inalámbrica
    - Tiene habilitado el servicio de VPNs *site to site* y VPN *Client*
    - Controla el enrutamiento a nivel WAN e Internet

- **Usuarios VPN:** Estos usuarios se pueden conectar de forma remota a consumir servicios internos de la Clínica a través de VPN Client. Estos usuarios se autentican a través del directorio activo de la organización.

- **Switch de Distribución:** Estos dispositivos definen y controlan VLANs de capa 2 y capa 3. Permite la configuración de puertos de acceso y los puertos troncales los cuales tiene el protocolo STP habilitado. Adicional se tienen implementados ACLs para controlar el tráfico y acceso a los dispositivos LAN.

- **Switch de Acceso:** Permiten la creación de vVLANs en capa 2. Se tiene habilitado el Port Security en los puertos de acceso de usuarios con almacenamiento de Log. Se tiene habilitado el protocolo STP.

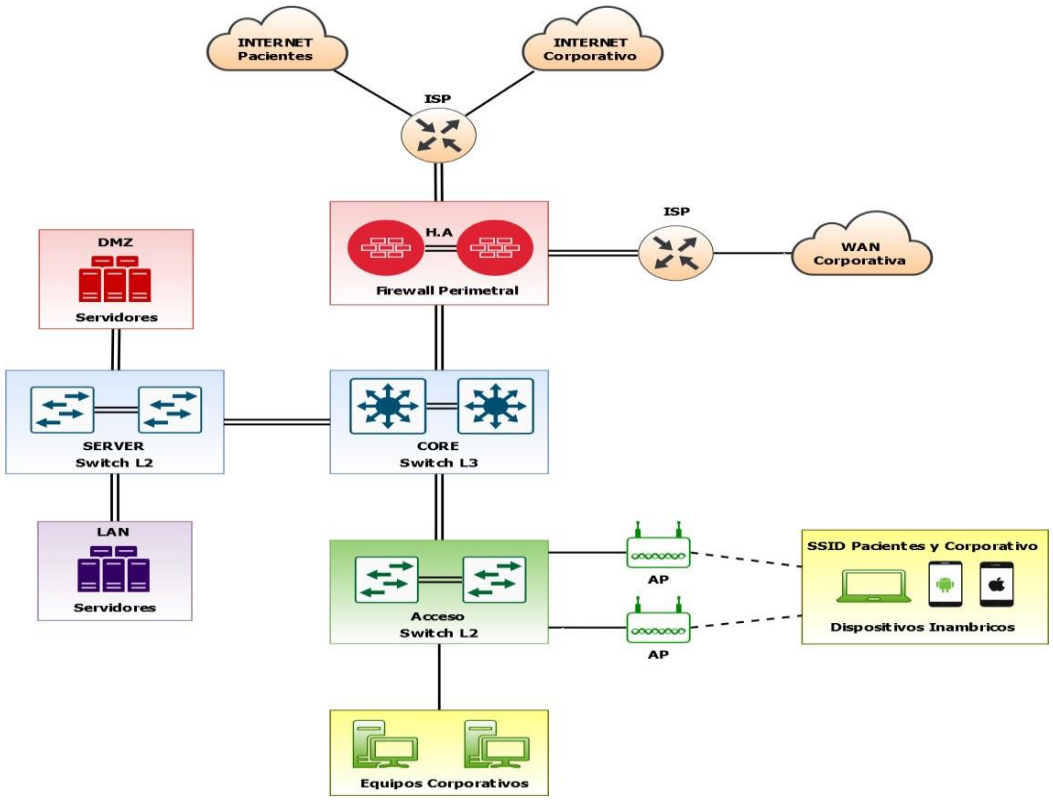
- **Servidores:** Tienen habilitado el Firewall Local y cuentan con un antivirus instalado local mente el cual es administrado en una consola centralizada. Adicional se tienen algunos controles de seguridad para las aplicaciones instaladas.

- **Estaciones de Trabajo:** Tienen habilitado el Firewall Local y cuentan con un antivirus instalado local mente el cual es administrado en una consola centralizada.
- **Red Inalámbrica:** La red inalámbrica cuenta con dispositivos Access point los cuales son controlados de forma centralizada a través de un módulo configurado en el Firewall Perimetral. La red WiFi tiene configurada 2 SSID (Empleados e Invitados – Pacientes) los cuales son independientes entre sí, con el fin de no permitir tráfico entre las redes. Adicional se cuenta con un portal cautivo en donde se solicita el acceso de un usuario y contraseña autorizados para permitir la navegación.

7.1.3 Diagrama topología de red documentada por el área de infraestructura de la clínica.

A continuación, en la ilustración 1, se observa el diagrama de topología de red documentada por el área de infraestructura de la clínica.

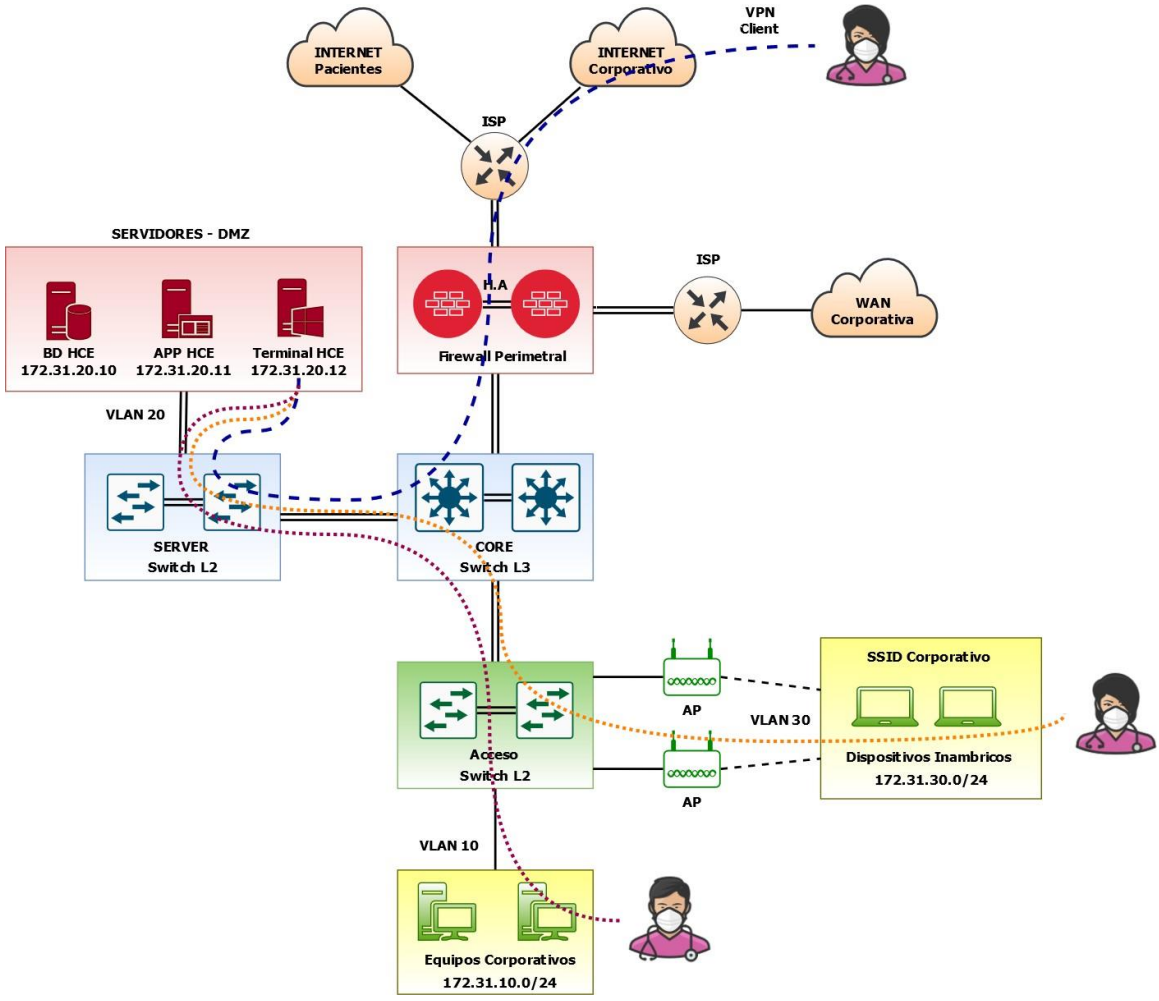
Ilustración 1. Diagrama de topología de red documentada por el área de infraestructura de la clínica



Fuente: elaboración propia

7.1.4 Diagrama topología de red con el levantamiento de información realizado. Al realizar el análisis de la información recolectada se evidencia que solo se tiene una VLAN de servidores, la cual es utilizada como DMZ para proveer servicios a los usuarios internos corporativos y a los usuarios que consumen recursos a través de internet de forma remota. A continuación, en la ilustración 2, se evidencia el diagrama de red con el flujo de información de acuerdo con el análisis realizado con la documentación recolectada:

Ilustración 2. Diagrama de topología de red analizada con el levantamiento de información realizado



Fuente: elaboración propia

7.1.5 Planes de Contingencia del aplicativo de historia clínica electrónica. Actualmente la clínica solo cuenta con un plan de contingencia manual, que consta de escribir en físico las ordenes, medicamentos y demás tratamiento de los pacientes, para los casos que haya interrupción en la aplicación de historia clínica electrónica.

7.1.6 Vías de ataque identificadas. Al realizar entrevistas acerca de la seguridad implementada en los dispositivos de red, servidores, maquinas cliente, bases de datos y aplicación de historia clínica electrónica al equipo de TI, se identifican las siguientes vías de ataque:

- La Clínica no cuenta con un procedimiento definido para realizar las actualizaciones de los dispositivos de red de forma periódica. Un atacante puede aprovechar una vulnerabilidad critica en los sistemas de red y explotarla, debido a que no se ha aplicado el parche de seguridad publicado por el fabricante.

  La versión del *Firewall* Fortigate cuenta en la actualidad con una versión de FortiOS 5.6.9. Al validar las posibles vulnerabilidades para este tipo de versión se identifica el CVE-2018-13383 de criticidad Alta.[28]

  CVE-2018-13383, una vulnerabilidad de desbordamiento de buffer de almacenamiento dinámico en el portal web FortiOS SSL VPN puede provocar la finalización del servicio web para los usuarios registrados o la posible ejecución remota de código en FortiOS. Esto sucede cuando un usuario autenticado visita una página web específicamente diseñada dando paso a una falla en el manejo adecuado de los datos href de JavaScript que son intermediados por un servidor proxy. Esto solo afecta al “modo web” SSL VPN (el modo túnel SSL VPN no se ve afectado), dando bases para un ataque de Denegación de Servicio ejecutado por código remoto.[29]

[28] CYBERSECURE. FORTINET informa vulnerabilidades detectadas en sus productos. [Sitio web]. Colombia:[Consulta: 20 de abril 2020]. Disponible en https://portal.cci-entel.cl/Threat_Intelligence/Boletines/361/

[29] NIST. CVE-2018-13383 Detail. [Sitio web]. Colombia:[Consulta: 20 de abril 2020]. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2018-13383

- La Clínica no cuenta con una política de contraseñas seguras para HCE, para la conexión a la base de datos ODBC y para el acceso a la aplicación a través de terminal server.

  Los posibles ataques en los que se pueden ver comprometidas las credenciales de los usuarios son:
  Ataques de Diccionario, que consisten en intentar autenticarse de forma continua a los sistemas, tomando posibles contraseñas de una base de datos creada.
  Ataques de Fuerza Bruta, utiliza la misma metodología de un ataque de diccionario, con la diferencia que este se genera dependiendo de la cantidad de posibles combinaciones.

- Algunas estaciones de trabajo no tienen aplicadas los KB descargadas debido a que estos equipos no se reinician constantemente.

  Al no aplicarse de forma pertinente los KB de actualización en las máquinas de trabajo, hace que una vulnerabilidad esté activa en el tiempo y pueda ser explotada.

- Todos los usuarios administrativos y asistenciales cuentan con permisos para descargar historias clínicas a la maquina local.

Esta mala práctica pone en riesgo la confidencialidad de la información y puede ser aprovechada por un atacante al explotar una vulnerabilidad en el sistema operativo de la maquina cliente, ingresar a ella y extraer esta información que contiene datos sensibles y confidenciales de los pacientes.

- Los servidores que están expuestos a internet se encuentran en la misma VLAN de los servidores internos (Bases de datos, historia clínica electrónica, aplicaciones, servidor de archivos, entre otros).

A través de vulnerabilidades que puedan presentar estos servidores expuestos a internet, se pueden producir ataques de código remoto afectando a todos los servidores que están en la misma VLAN, debido a que no existe una barrera (Firewall) que impida el acceso a otros servidores no autorizados.

- La clínica no maneja guías de *hardening* para el alistamiento de dispositivos nuevos en la red.

Al no existir guías de *hardening* para el alistamiento de los dispositivos, no es posible asegurar que se cumplan buenas prácticas como deshabilitar protocolos inseguros, inhabilitar servicios que no se utilizan, eliminar usuarios y contraseñas por defecto, entre otros, estas provocan vulnerabilidades que pueden convertirse en ataques fácilmente.

- La conexión VPN no cuenta con un certificado digital confiable.

Al no contar con un certificado digital en la comunicación entre el Firewall y el equipo cliente de la VPN, la información no cuenta con cifrado robusto de extremo a extremo que este avalado por una entidad certificadora a nivel mundial, ocasionando vulnerabilidades y exposición a ataques de suplantación de identidad.

- La conexión VPN no cuenta con doble factor de autenticación

Al no contar con doble factor de autenticación, está expuesto a ataques de *phishing* e ingeniería social, donde el atacante al lograr obtener el usuario y la contraseña puede ingresar a los sistemas sin ser detectado.

- El usuario y la contraseña es la misma para la conexión de la base de datos (ODBC), adicional la información de esta configuración no se encuentra cifrada.

Esta vulnerabilidad es crítica porque un atacante puede obtener por medio de un *sniffer* (Wireshark), los datos de la conexión ODBC que viajan en texto plano desde el servidor terminal hacia la base de datos cada vez que se realiza un *login* a la aplicación de historia clínica electrónica y con estos datos de conexión puede acceder al servidor donde se encuentra almacenada la base de datos.

Al realizar entrevistas al personal administrativo y asistencial acerca de las buenas prácticas que manejan en la aplicación de historia clínica electrónica, se identifican la siguiente vía de ataque:

- Préstamo de usuarios para el ingreso a la aplicación de Historia Clínica Electrónica entre los empleados.

Esta mala práctica pone en riesgo la confidencialidad e integridad de la información, debido a que no se puede tener un control verídico en cuanto a consulta, modificación o eliminación de datos sensibles y confidenciales. Un atacante puede recurrir a ataques de ingeniería social y realizar modificación o eliminación en la información sin ser detectado.

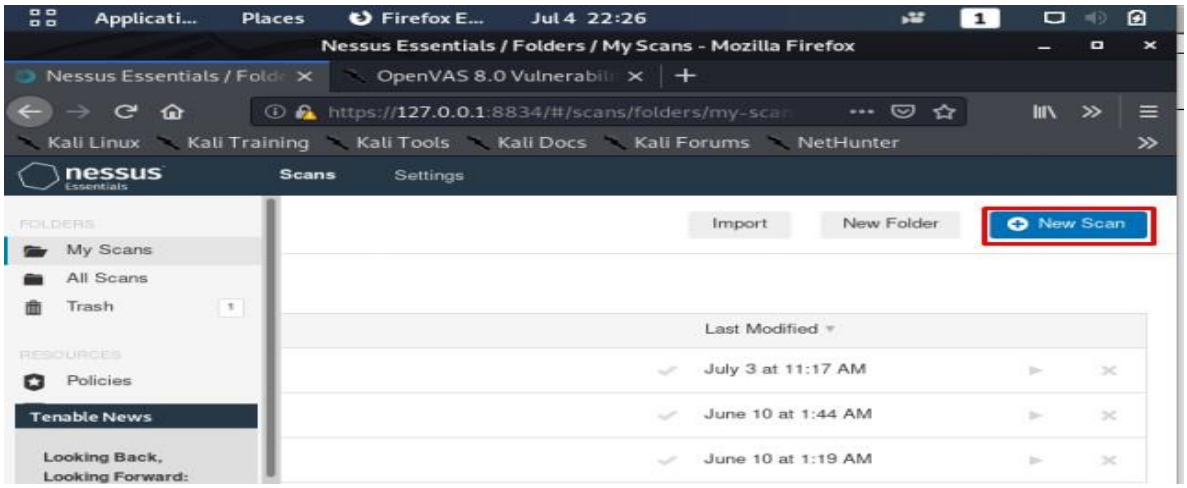
7.2 DESARROLLO DE OBJETVO 2: GENERAR UN ANÁLISIS DE VULNERABILIDADES EXISTENTES EN LA APLICACIÓN DE HISTORIA CLÍNICA ELECTRÓNICA A TRAVÉS DE UNA HERRAMIENTA DE SEGURIDAD INFORMÁTICA.

Para el desarrollo del objetivo 2 se utiliza la cuarta fase de la metodología PTES que consiste en realizar el análisis de vulnerabilidades, para esto se utiliza la herramienta Nessus, la cual consiste en un demonio (nessusd) que realiza un escaneo de puertos abiertos en el sistema objetivo e intenta varios *exploits* para atacarlo y una interfaz gráfica (nessus) que muestra e informa el estado del escaneo, las vulnerabilidades existentes, el CVE asociado y la forma de dar solución o mitigar la vulnerabilidad[30]

A continuación, se detalla el proceso efectuado para el escaneo de los diferentes dispositivos de red en los diferentes dispositivos de red que hacen parte de la aplicación de Historia Clínica Electrónica:

Se da clic en el botón *New Scan* para generar un nuevo escaneo de vulnerabilidades, como se puede observar en la Figura 3.

Ilustración 3. Nuevo escaneo en la herramienta Nessus

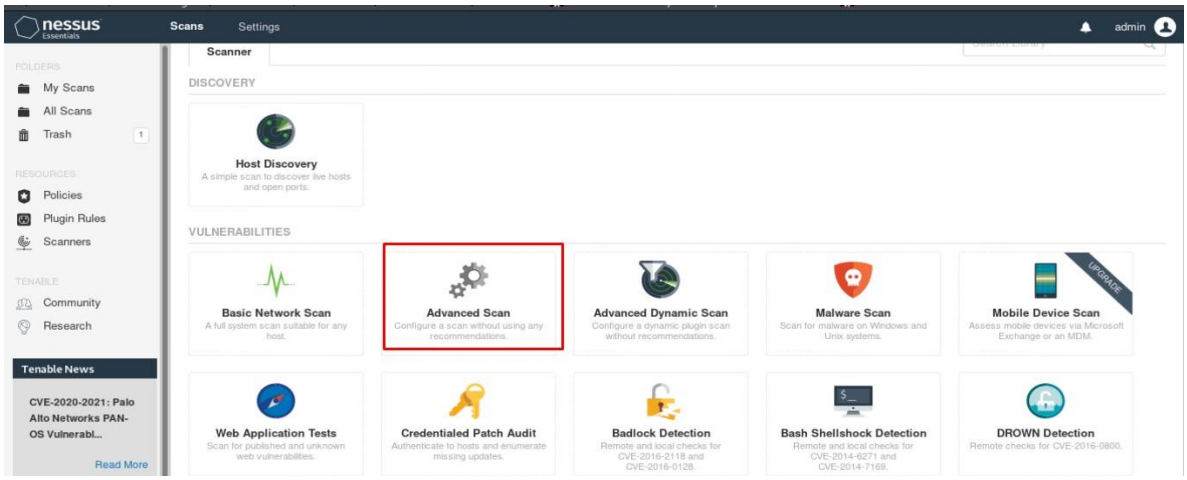


Fuente: elaboración propia

[30] MUNDO HACKERS. Nessus. [Sitio web]. Colombia: [Consulta: 28 de abril 2020]. Disponible en https://mundo-hackers.weebly.com/nessus.html

Se selecciona el tipo de escaneo: *Advanced Scan*, como se puede observar en la Figura 4.

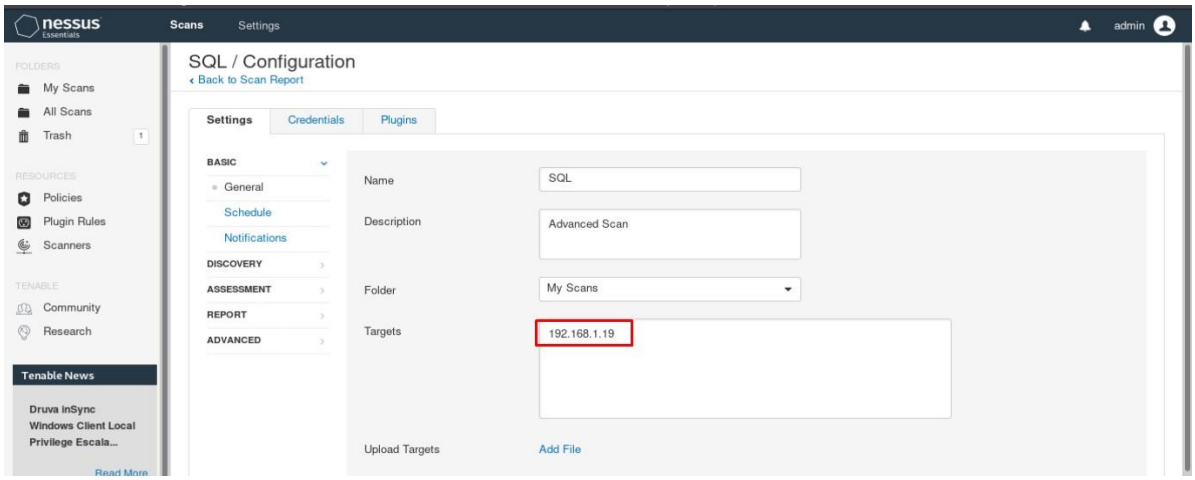
Ilustración 4. *Advance Scan* Nessus



Fuente: elaboración propia

Se coloca el nombre para identificar el escaneo, la dirección IP del servidor o sistema a analizar, como se puede observar en la Figura 5.

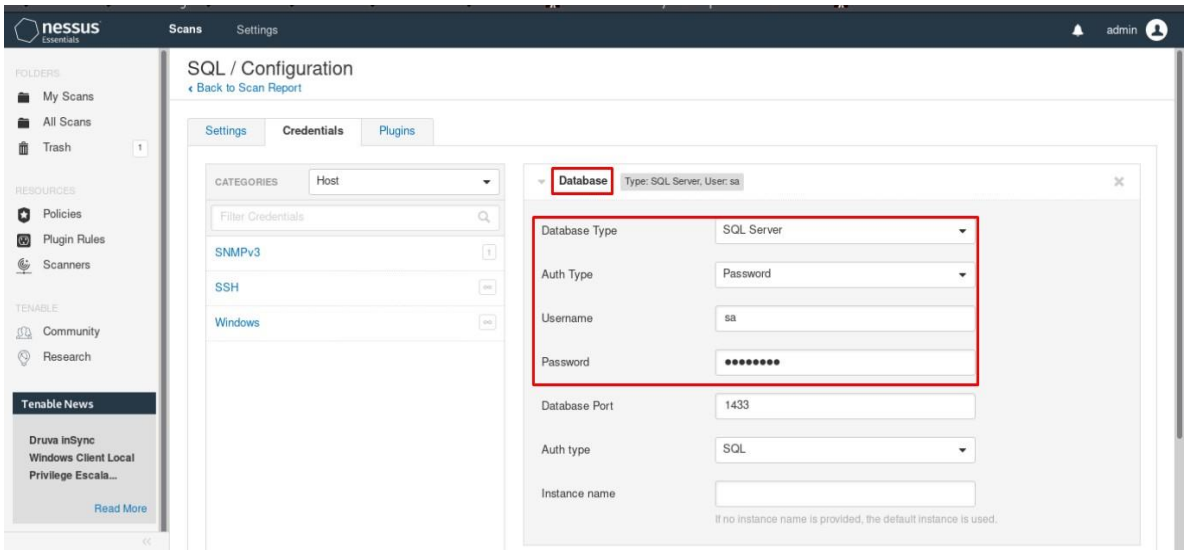
Ilustración 5. IP del sistema a analizar Nessus



Fuente: elaboración propia

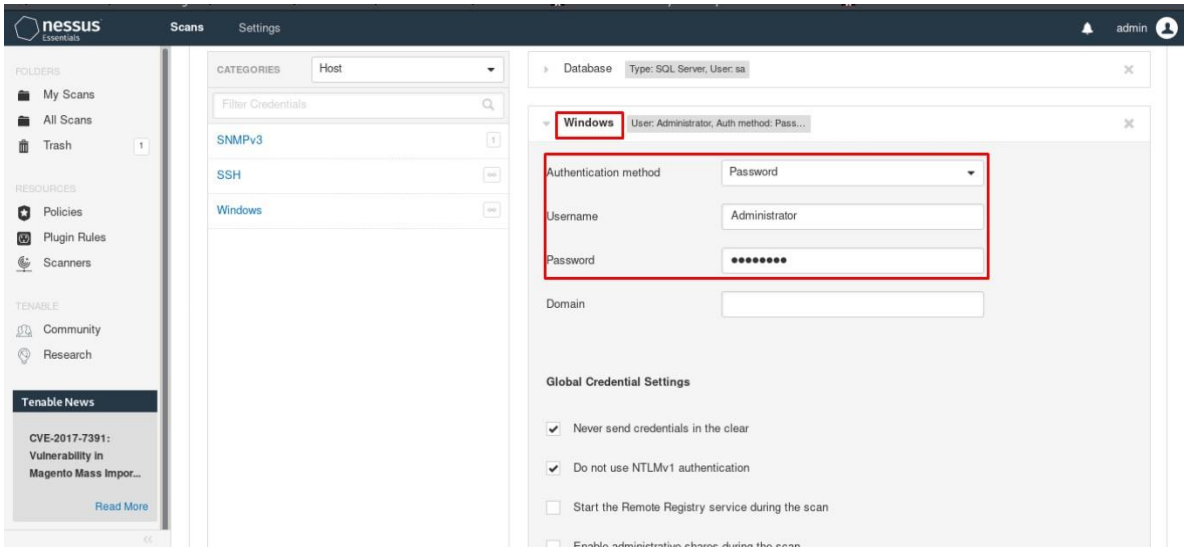
Se puede agregar usuario y contraseña del sistema operativo y demás, para obtener más información al momento de generar el escaneo de vulnerabilidades, como se puede observar en la Figura 6 y Figura 7.

Ilustración 6. Usuario y contraseña del dispositivo de red Nessus



Fuente: elaboración propia

Ilustración 7. Usuario y contraseña del dispositivo de red Nessus



Fuente: elaboración propia

Al finalizar el escaneo, la herramienta Nessus muestra un informe con todas las vulnerabilidades encontradas tanto en el sistema operativo, bases de datos, firewall, aplicaciones web existentes y demás dispositivos de la red de la Clínica que hacen parte de la historia clínica electrónica.

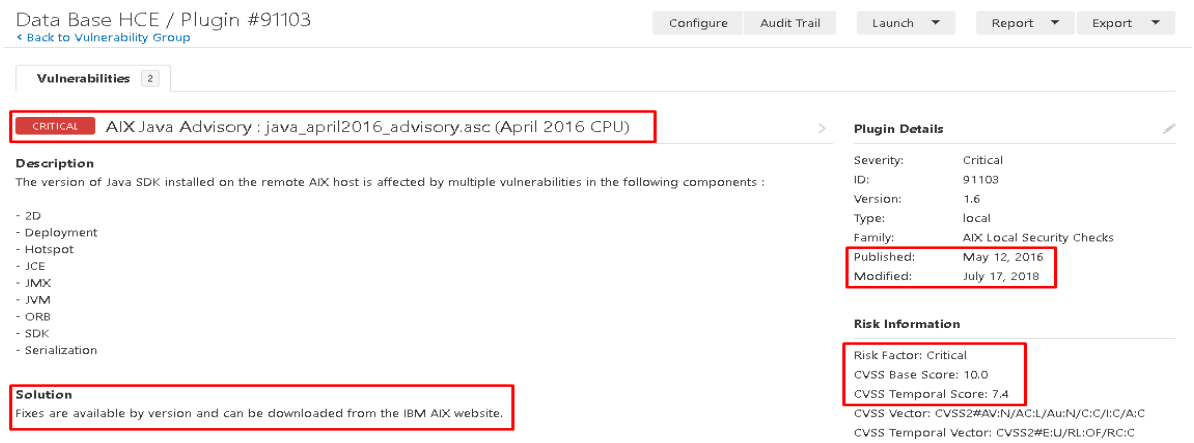
A continuación, se listan las vulnerabilidades encontradas en los diferentes dispositivos de red:

7.2.1 Servidor base de datos. A continuación, se pueden observar las vulnerabilidades encontradas en el servidor de base de datos, el CVE relacionado y la solución indicada para mitigar una posible intrusión.

- **Vulnerabilidad de AIX Java.**

La versión de Java SDK instalada en el host AIX remoto se ve afectada por múltiples vulnerabilidades en los siguientes componentes: 2D, deployment, hospot, JCE, SDK y serialización, permitiendo a un atacante remoto saltar las medidas de aseguramiento de un espacio e introducir código malicioso.[31] Los CVE relacionados son: CVE-2016-0264 CVE-2016-0363 CVE-2016-0376 CVE-2016-0686 CVE-2016-0687 CVE-2016-3422 CVE-2016-3426 CVE-2016-3427 CVE-2016-3443 CVE-2016-3449, como se puede observar en la Figura 8.

Ilustración 8. Vulnerabilidad de AIX Java.



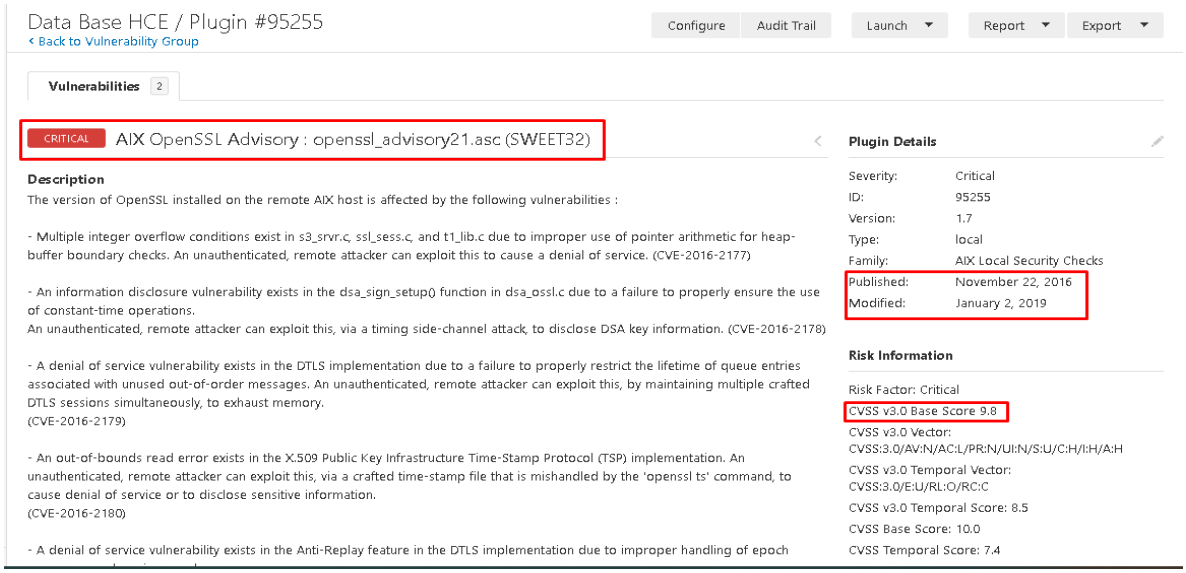
Fuente: elaboración propia

[31] NIST. Base de datos nacional de vulnerabilidades. [Sitio web]. Colombia: [Consulta: 06 de noviembre 2020]. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2016-0264

- **Vulnerabilidad de AIX Open SSL.**

La versión de OPENSSL instalada en el host remoto AIX esta desactualizada, permitiendo a un atacante remoto un ataque de denegación de servicio por medio de un archivo corrupto llamado OPENSSL TS.[32] Los CVE relacionados son: CVE-2016-2177 CVE-2016-2178 CVE-2016-2179 CVE-2016-2180 CVE-2016-2181 CVE-2016-2182 CVE-2016-2183 CVE-2016-6302 CVE-2016-6303 CVE-2016-6304 CVE-2016-6306 CVE-2016-7052, como se puede observar en la Figura 9.

Ilustración 9. Vulnerabilidad de AIX Open SSL



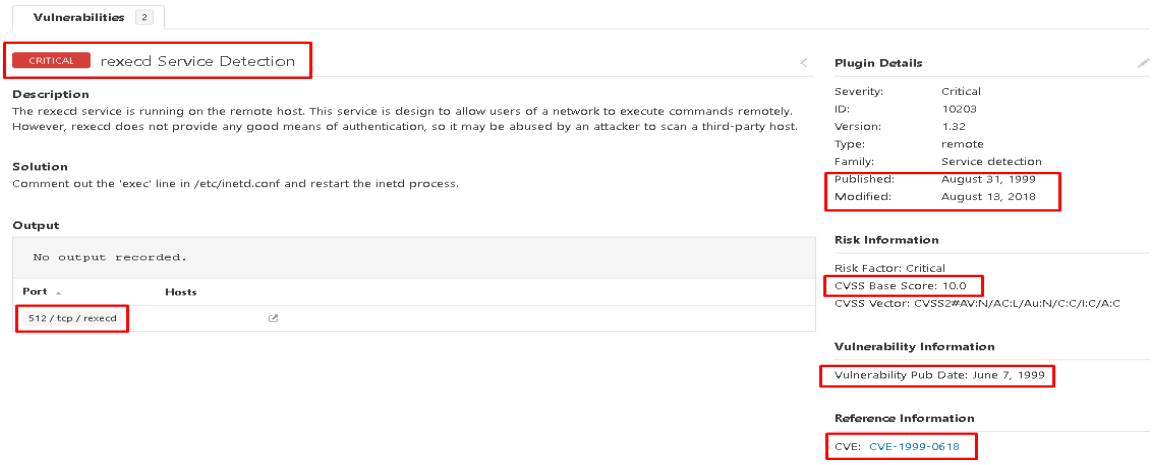
Fuente: elaboración propia

- **Vulnerabilidad Rexecd Service.**

El servicio Rexecd se encuentra en ejecución por el protocolo TCP y el puerto 512, permitiendo a un atacante remoto ejecución de código malicioso.[33] El CVE relacionado es: CVE-1999-0618, como se puede observar en la Figura 10.

[32] NIST. Base de datos nacional de vulnerabilidades. [Sitio web]. Colombia: [Consulta: 06 de noviembre 2020]. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2016-2177
[33] NIST. Base de datos nacional de vulnerabilidades. [Sitio web]. Colombia: [Consulta: 06 de noviembre 2020]. Disponible en https://nvd.nist.gov/vuln/detail/CVE-1999-0618

Ilustración 10. Vulnerabilidad Rexecd Service

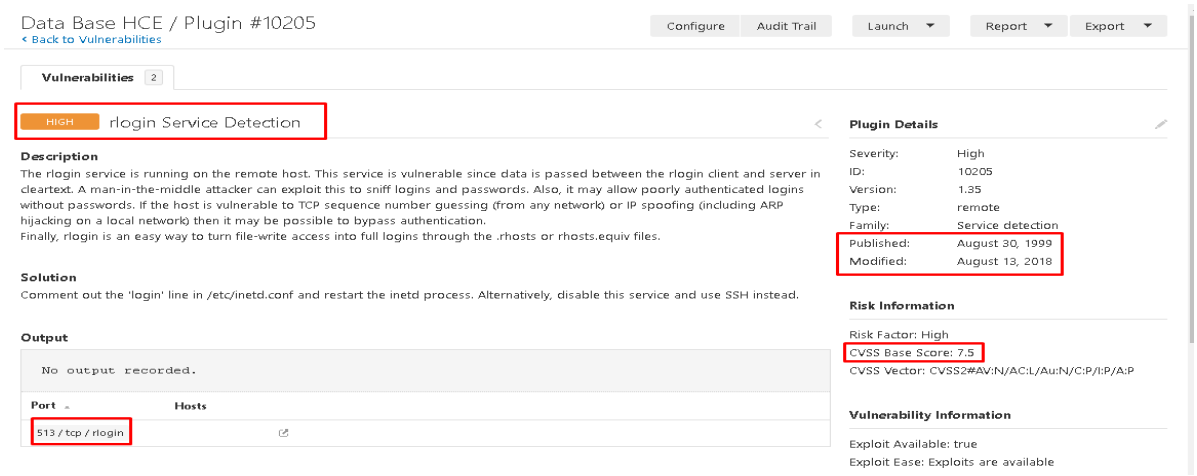


Fuente: elaboración propia

- **Vulnerabilidad rlogin Service.**

El servicio rlogin se encuentra en ejecución por el protocolo TCP y el puerto 513, permitiendo a un atacante remoto ejecución de código malicioso.[34] El CVE relacionado es: CVE-1999-0651, como se puede observar en la Figura 11.

Ilustración 11. Vulnerabilidad rlogin Service



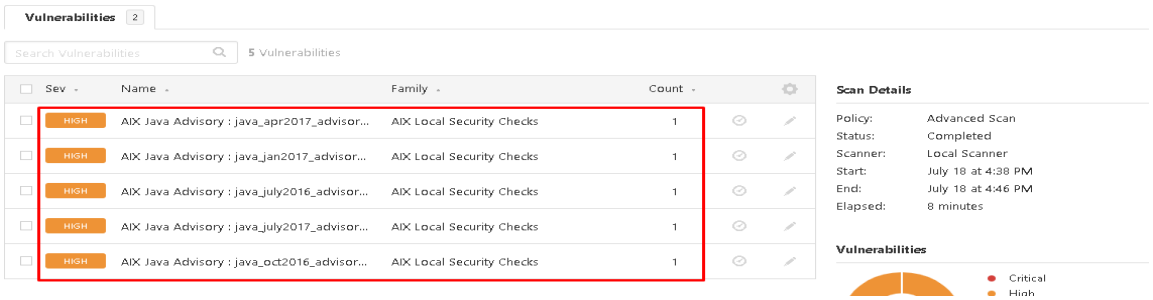
Fuente: elaboración propia

[34] NIST. Base de datos nacional de vulnerabilidades. [Sitio web]. Colombia: [Consulta: 06 de noviembre 2020]. Disponible en https://nvd.nist.gov/vuln/detail/CVE-1999-0651

- **Vulnerabilidades asociadas a la versión de Java instalada en el servidor AIX.**

A continuación, se puede observar en la Figura 12 un resumen de las vulnerabilidades altas con respecto a la versión de java instalado en el servidor de base de datos.

Ilustración 12. Vulnerabilidad Java

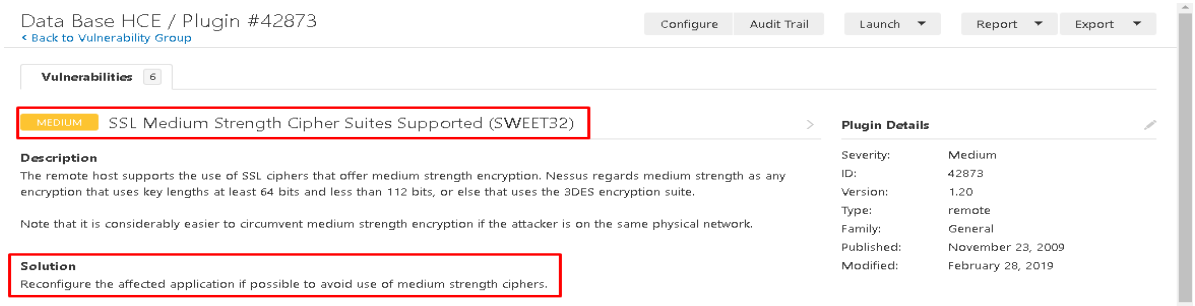


Fuente: elaboración propia

- **Vulnerabilidad Cipher Suites SSL.**

Los métodos de cifrado DES y triple DES utilizados en los protocolos de comunicación TLS, SSH E IPSec son inseguros, permitiendo a un atacante remoto obtener datos en texto claro. [35] El CVE relacionado es: CVE-2016-2183, como se puede observar en la Figura 13.

Ilustración 13. Vulnerabilidad Cipher Suites SSL



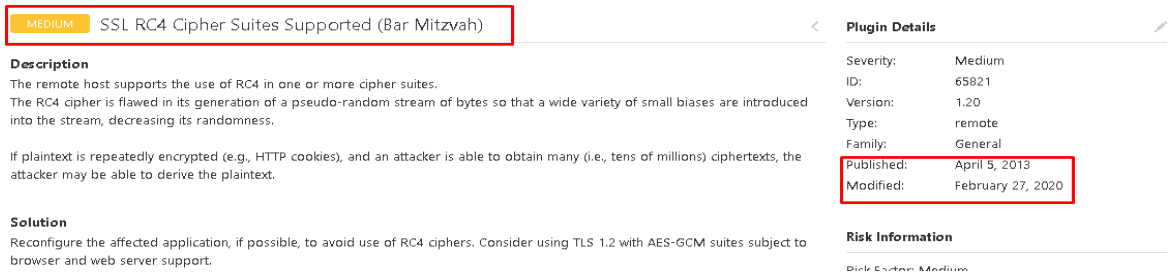
Fuente: elaboración propia

[35] NIST. Base de datos nacional de vulnerabilidades. [Sitio web]. Colombia: [Consulta: 06 de noviembre 2020]. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2016-2183

- **Vulnerabilidad Cipher Suites SSL RC4.**

El algoritmo RC4 utilizado en los protocolos TLS y SSL no se encuentra correctamente cifrado, permitiendo a un atacante remoto un ataque de recuperación de texto.[36] CVE relacionados: CVE-2013-2566 CVE-2015-2808, como se puede observar en la Figura 14.

Ilustración 14. Vulnerabilidad Cipher Suites SSL RC4

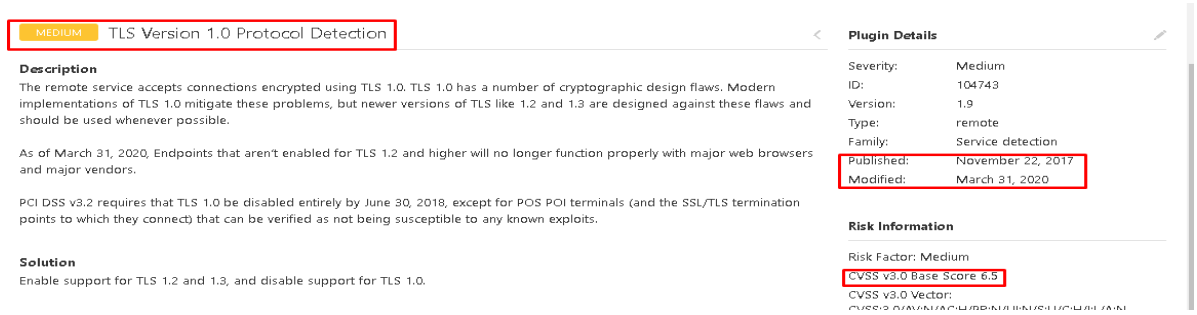


Fuente: elaboración propia

- **Vulnerabilidad TLS Versión 1.0**

El servicio remoto acepta conexiones cifradas con TLS 1.0. TLS 1.0 tiene una serie de defectos de diseño criptográfico, como se puede observar en la Figura 15.

Ilustración 15. Vulnerabilidad TLS Versión 1.0

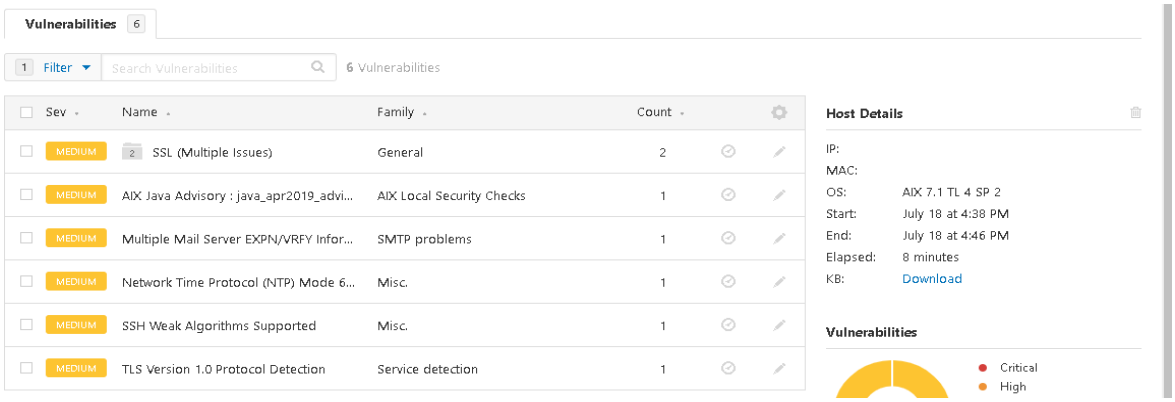


Fuente: elaboración propia

[36] NIST. Base de datos nacional de vulnerabilidades. [Sitio web]. Colombia: [Consulta: 06 de noviembre 2020]. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2015-2808

A continuación, se puede observar en la Figura 16 un resumen de las vulnerabilidades medias en el servidor de base de datos.

Ilustración 16. Resumen vulnerabilidades medias base de datos



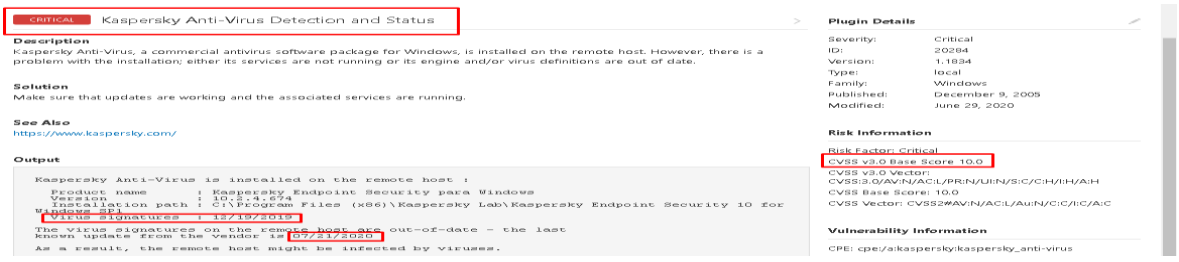
Fuente: elaboración propia

7.2.2 Servidor Terminal Server HCE. A continuación, se pueden observar las vulnerabilidades encontradas en el servidor terminal server HCE, el CVE relacionado y la solución indicada para mitigar una posible intrusión.

- **Vulnerabilidad Antivirus Kaspersky.**

El antivirus Kaspersky que se encuentra instalado en el servidor no está ejecutando el motor o las firmas están desactualizadas, permitiendo que un atacante pueda ejecutar código malicioso e infectar los dispositivos de la red, como se puede observar en la Figura 17.

Ilustración 17. Vulnerabilidad Antivirus Kaspersky

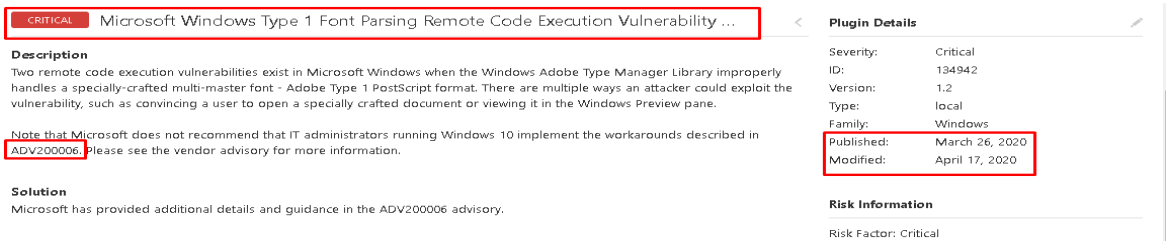


Fuente: elaboración propia

- **Vulnerabilidad Ejecución código remoto.**

La biblioteca de Adobe Type Manager maneja incorrectamente una fuente multimaestro especialmente diseñada, permitiendo a un a un atacante remoto convencer a un usuario para que abra un documento o lo visualice en el panel de vista previa de Windows, como se puede observar en la Figura 18.

Ilustración 18. Vulnerabilidad Ejecución código remoto

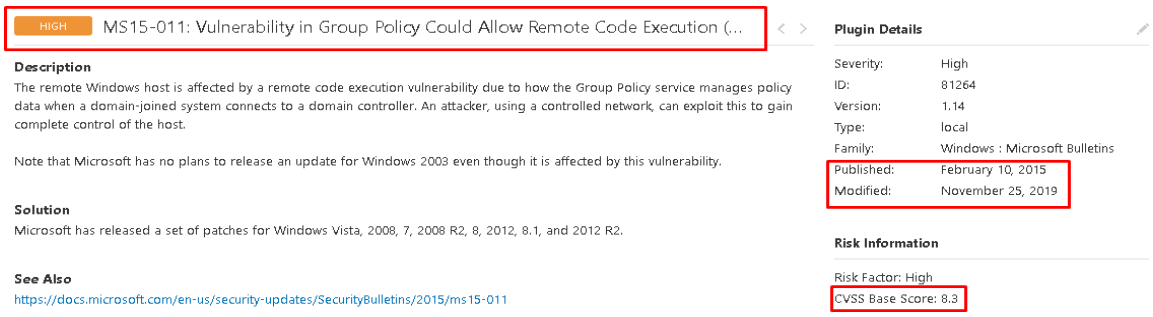


Fuente: elaboración propia

- **Vulnerabilidad de código remoto.**

La implementación de UNC en Microsoft Windows Server 2003 SP2 no incluye autenticación de del servidor al cliente, permitiendo a un atacante remoto ejecutar código arbitrario haciendo que los datos creados estén disponibles en un recurso compartido de UNC.[37] El CVE relacionado es: CVE-2015-0008, como se puede observar en la Figura 20.

Ilustración 19. Vulnerabilidad de código remoto



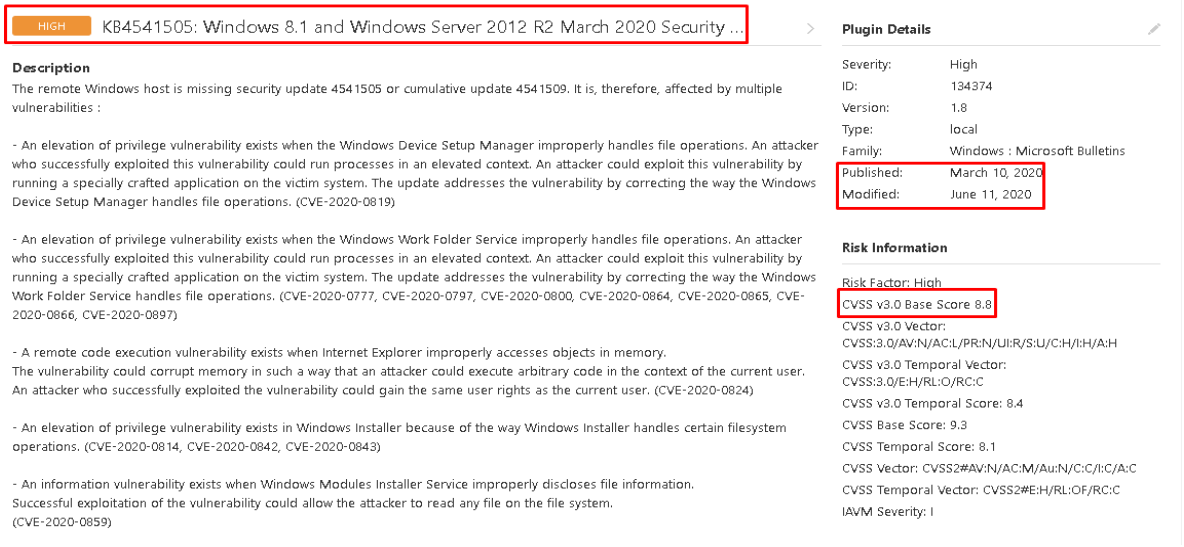
Fuente: elaboración propia

[37] NIST. Base de datos nacional de vulnerabilidades. [Sitio web]. Colombia: [Consulta: 06 de noviembre 2020]. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2015-0008

- **Vulnerabilidad de actualización acumulativa.**

A continuación, se puede observar en la Figura 20 las vulnerabilidades acumulativas del Servidor Terminal Server HCE. Los CVE relacionados son: CVE-2020-0645, CVE-2020-0684, CVE-2020-0768 al CVE-2020-0774, CVE-2020-0770 al CVE-2020-0781, CVE-2020-0783 al CVE-2020-0785, CVE-2020-0787, CVE-2020-0788, CVE-2020-0791, CVE-2020-0797, CVE-2020-0799, CVE-2020-0800, CVE-2020-0802 al CVE-2020-0804, CVE-2020-0806, CVE-2020-0814, CVE-2020-0814, CVE-2020-0822,CVE-2020-0824, CVE-2020-0830, CVE-2020-0832 al CVE-2020-0834, CVE-2020-0840, CVE-2020-0842 al CVE-2020-0845, CVE-2020-0847, CVE-2020-0849, CVE-2020-0853, CVE-2020-0857 al CVE-2020-0861, CVE-2020-0864 al CVE-2020-0866, CVE-2020-0871, CVE-2020-0874, CVE-2020-0877, CVE-2020-0879 al CVE-2020-0883, CVE-2020-0885, CVE-2020-0887, CVE-2020-0897.

Ilustración 20. Vulnerabilidad de actualización acumulativa



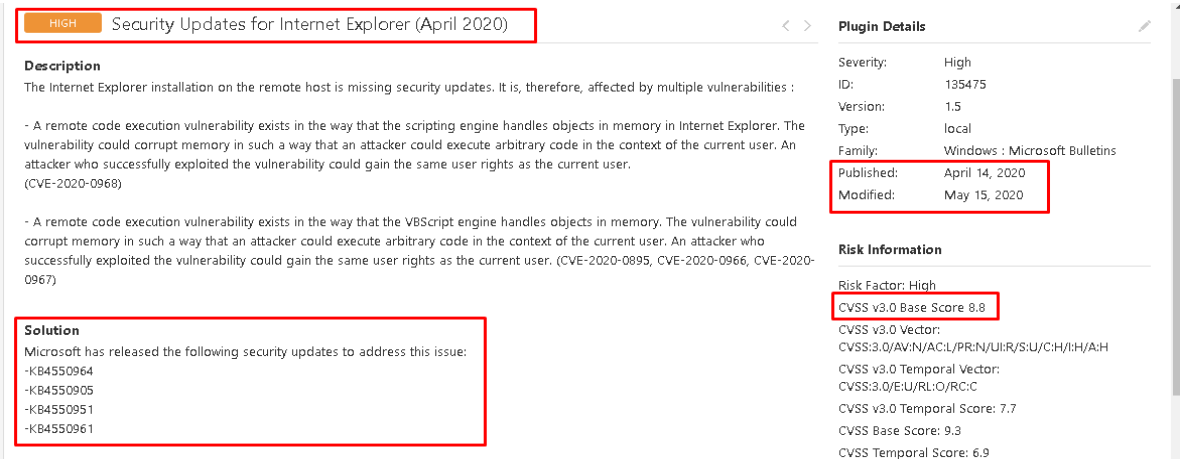
Fuente: elaboración propia

- **Vulnerabilidad actualización de internet explorer.**

La versión de internet Explorer se encuentra desactualizada y cuenta con vulnerabilidades, permitiendo que un atacante remoto aproveche las vulnerabilidades para ejecutar código malicioso en el motor de comando de los

objetos de memoria del IE.[38] Los CVE relacionados son: CVE-2020-0895, CVE-2020-0966 al CVE-2020-0968, como se puede observar en la Figura 21.

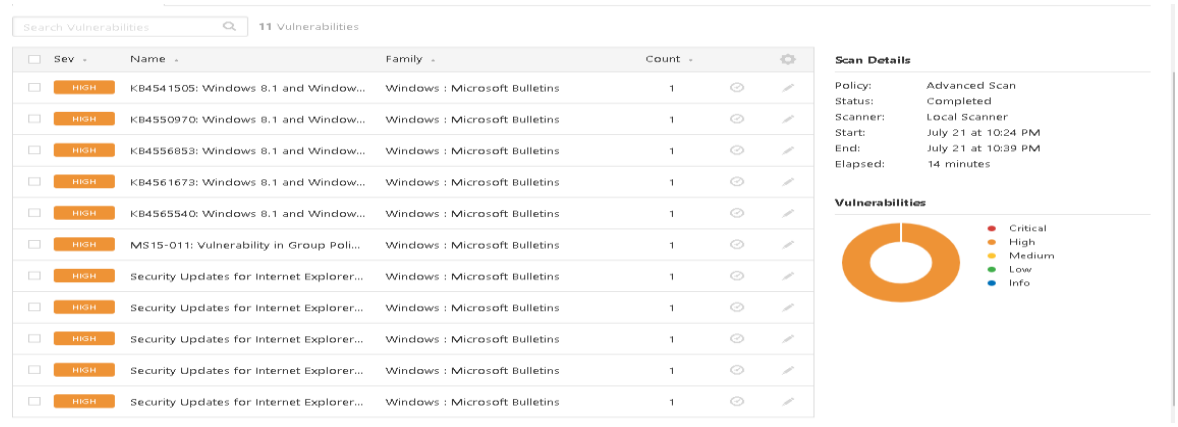
Ilustración 21. Vulnerabilidad actualización de internet explorer



Fuente: elaboración propia

A continuación, se puede observar en la Figura 22 un resumen de las vulnerabilidades altas en el servidor terminal server HCE.

Ilustración 22. Resumen vulnerabilidades en el servidor de terminal server



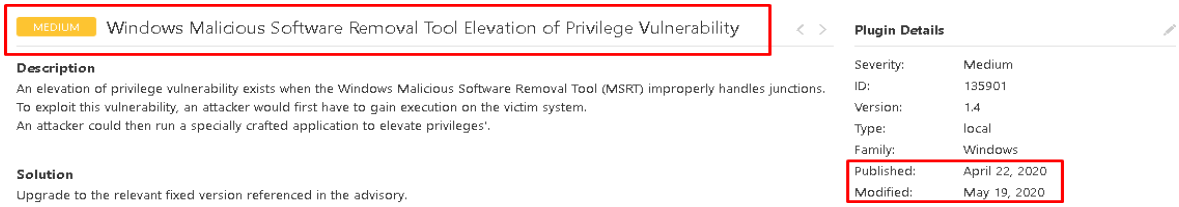
Fuente: elaboración propia

[38] NIST. Base de datos nacional de vulnerabilidades. [Sitio web]. Colombia: [Consulta: 06 de noviembre 2020]. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2020-0968

- **Vulnerabilidad de elevación de permisos.**

Existe una vulnerabilidad de elevación de privilegios cuando la Herramienta de eliminación de software malintencionado de Windows maneja incorrectamente las uniones, permitiendo a un atacante elevar permisos después de un ataque.[39] El CVE relacionado es: CVE-2020-0733, como se puede observar en la Figura 23.

Ilustración 23. Vulnerabilidad de elevación de permisos

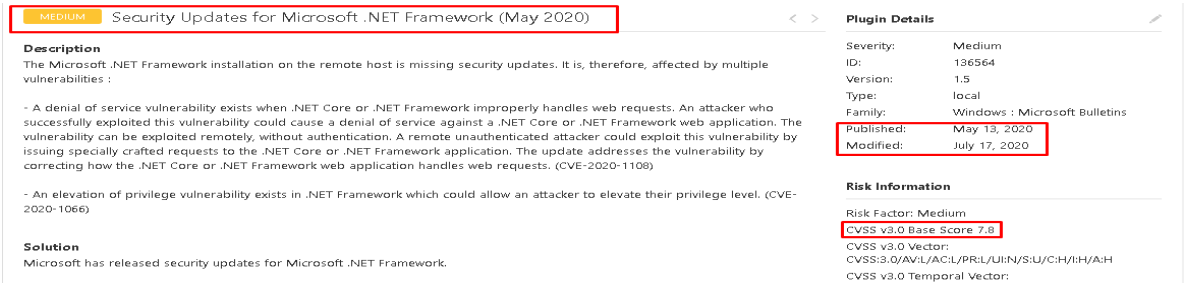


Fuente: elaboración propia

- **Vulnerabilidad de .Net Framework.**

La versión del Net Framework se encuentra desactualizada, permitiendo a un atacante remoto introducir código malicioso. [40] Los CVE relacionados son: CVE-2020-1066 CVE-2020-1108, como se puede observar en la Figura 24.

Ilustración 24. Vulnerabilidad de .Net Framework

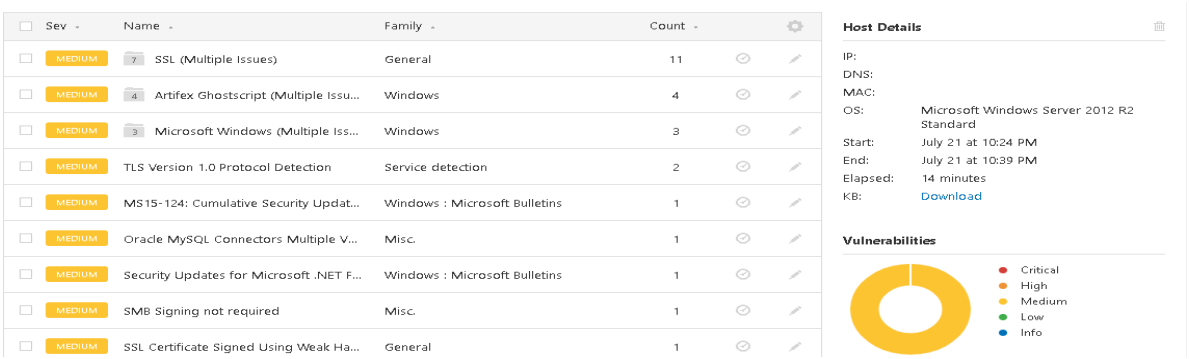


Fuente: elaboración propia

[39] NIST. Base de datos nacional de vulnerabilidades. [Sitio web]. Colombia: [Consulta: 06 de noviembre 2020]. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2020-0733
[40] NIST. Base de datos nacional de vulnerabilidades. [Sitio web]. Colombia: [Consulta: 06 de noviembre 2020]. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2020-1108

A continuación, se puede observar en la Figura 25 un resumen de las vulnerabilidades medias en el servidor terminal server HCE.

Ilustración 25. Resumen vulnerabilidades medias en el servidor de terminal server



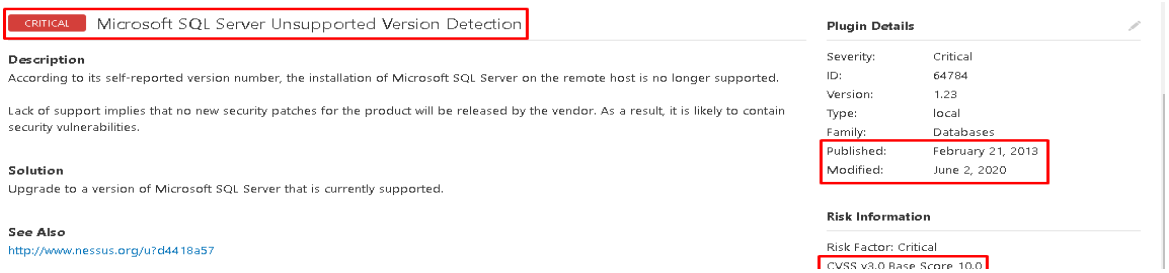
Fuente: elaboración propia

7.2.3 Servidor de Aplicación HCE. A continuación, se pueden observar las vulnerabilidades encontradas en el servidor de aplicación HCE, el CVE relacionado y la solución indicada para mitigar una posible intrusión.

- **Vulnerabilidad Microsoft SQL Server.**

La versión del SQL Server no cuenta con soporte por parte de Microsoft, permitiendo a aun atacante remoto ejecutar código malicioso, como se puede observar en la Figura 26.

Ilustración 26. Vulnerabilidad Microsoft SQL Server

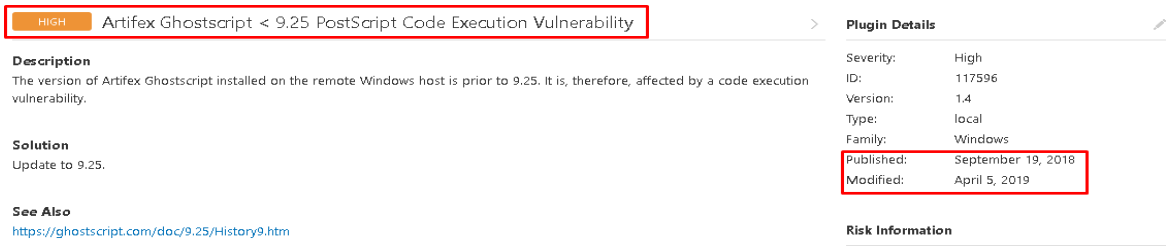


Fuente: elaboración propia

- **Vulnerabilidad de Artifex Ghostscript.**

la versión de artifex ghostscript instalada en el host de Windows remoto es anterior a la 9.25, permitiendo a un atacante remoto ejecución de código malicioso. [41] Los CVE relacionados son: CVE-2018-16509 CVE-2018-16802, como se puede observar en la Figura 27.

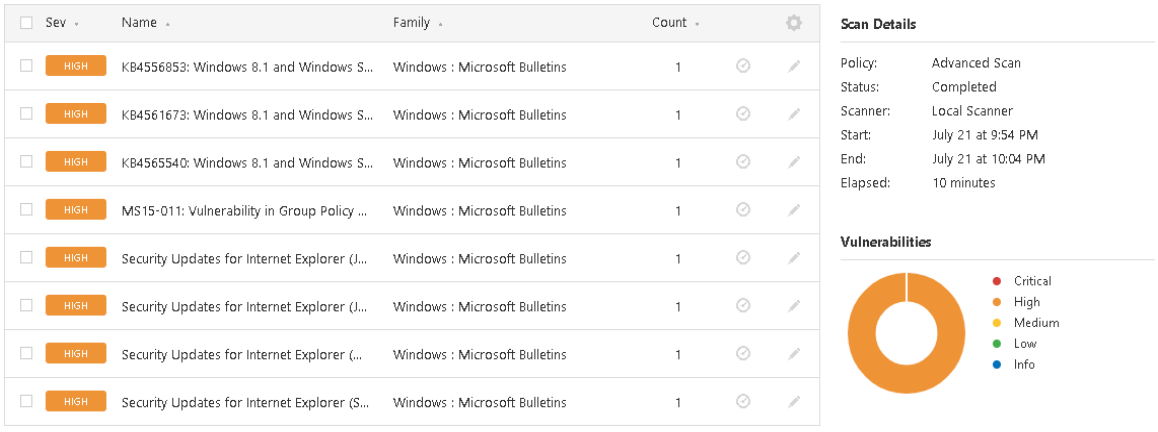
Ilustración 27. Vulnerabilidad de Artifex Ghostscript



Fuente: elaboración propia

A continuación, se puede observar en la Figura 28 un resumen de las vulnerabilidades altas en el servidor de aplicación HCE.

Ilustración 28. Resumen vulnerabilidades altas en el servidor de aplicación



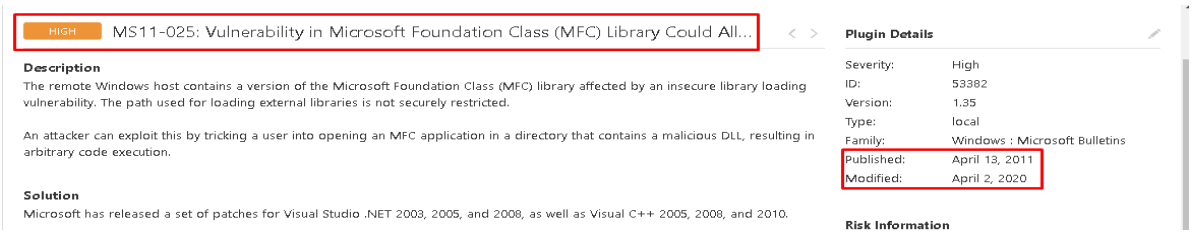
Fuente: elaboración propia

[41] NIST. Base de datos nacional de vulnerabilidades. [Sitio web]. Colombia: [Consulta: 06 de noviembre 2020]. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2018-16802

- **Vulnerabilidad MFC.**

Vulnerabilidad de ruta de búsqueda no confiable en la biblioteca Microsoft Foundation Class en Microsoft Visual Studio .NET, permitiendo a un atacante remoto ejecución de código malicioso.[42] El CVE relacionado es: CVE-2010-3190, como se puede observar en la Figura 29.

Ilustración 29. Vulnerabilidad MFC



Fuente: elaboración propia

- **Vulnerabilidad Remote desktop Man in the middle**

Microsoft Terminal Server que usa el Protocolo de escritorio remoto (RDP) que almacena una clave privada RSA y la usa para firmar un certificado, permitiendo a un atacante remote falsificar las claves públicas de servidores legítimos y realizar ataques man-in-the-middle.[43] El CVE relacionado es: CVE-2005-1794, como se puede observar en la Figura 30.

Ilustración 30. Vulnerabilidad Remote desktop Man in the middle

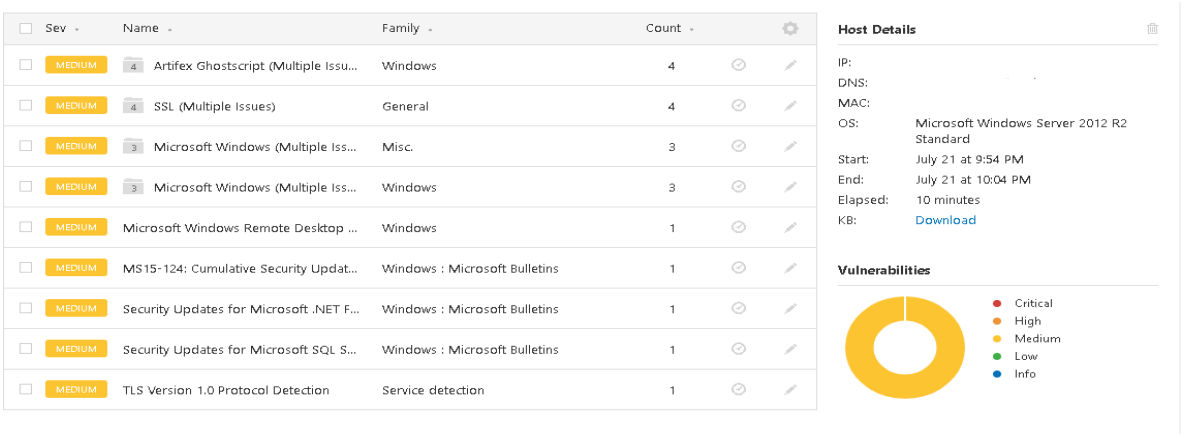
Fuente: elaboración propia

[42] NIST. Base de datos nacional de vulnerabilidades. [Sitio web]. Colombia: [Consulta: 06 de noviembre 2020]. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2010-3190

[43] NIST. Base de datos nacional de vulnerabilidades. [Sitio web]. Colombia: [Consulta: 06 de noviembre 2020]. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2005-1794

A continuación, se puede observar en la Figura 31 un resumen de las vulnerabilidades medias en el servidor de aplicación HCE.

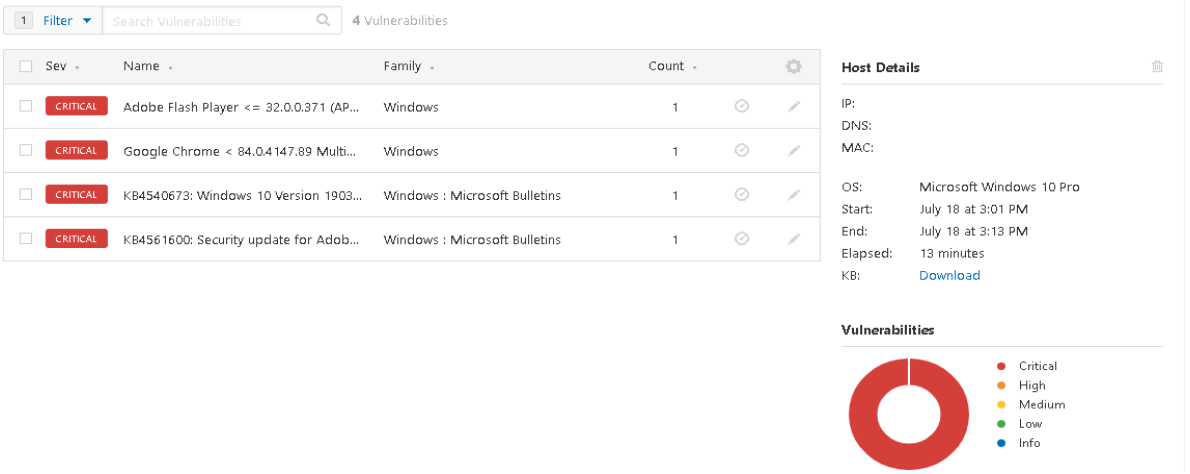
Ilustración 31. Resumen vulnerabilidades medias en el servidor de aplicación HCE.



Fuente: elaboración propia

7.2.4 Equipo Usuario Administrativo HCE Windows10. A continuación, se puede observar en la Figura 32 un resumen de las vulnerabilidades críticas en el equipo del usuario administrativo, el CVE relacionado y la solución indicada para mitigar una posible intrusión.

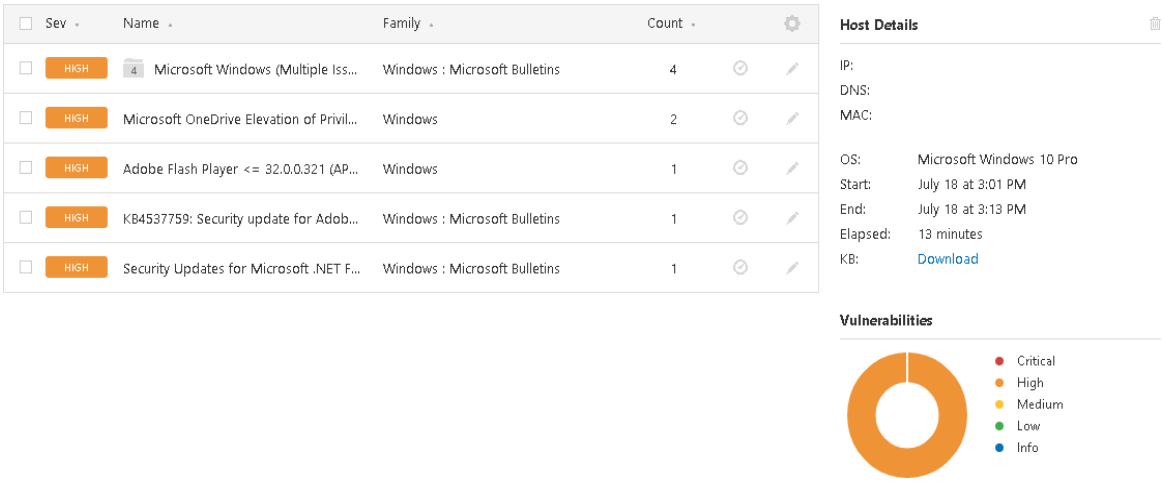
Ilustración 32. Resumen vulnerabilidades críticas en el equipo usuario administrativo



Fuente: elaboración propia

A continuación, se puede observar en la Figura 33 un resumen de las vulnerabilidades altas en el equipo del usuario administrativo.

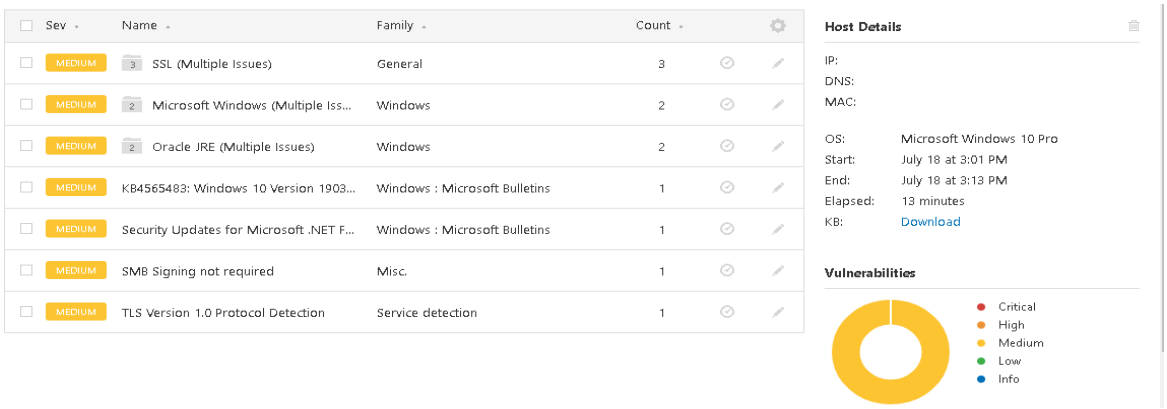
Ilustración 33. Resumen vulnerabilidades altas en el equipo usuario administrativo



Fuente: elaboración propia

A continuación, se puede observar en la Figura 34 un resumen de las vulnerabilidades medias en el equipo del usuario administrativo.

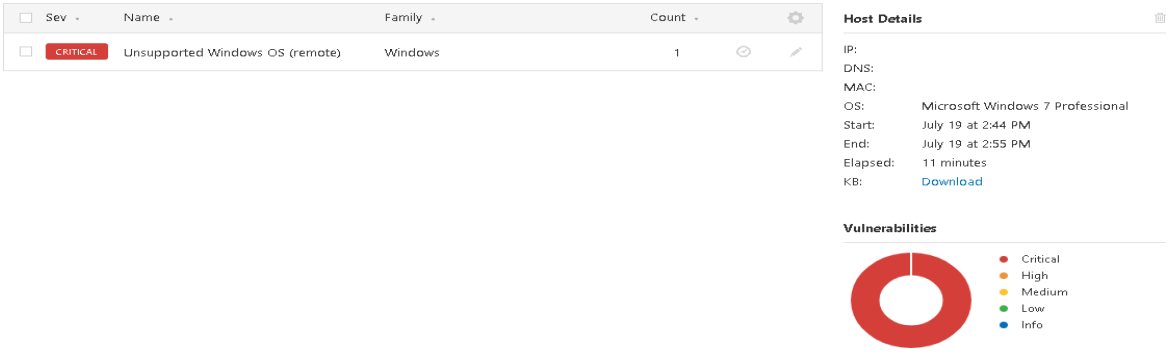
Ilustración 34. Resumen vulnerabilidades medias en el equipo usuario administrativo



Fuente: elaboración propia

7.2.5 Equipo Usuario Asistencial HCE Windows7. A continuación, se puede observar en la Figura 35 un resumen de las vulnerabilidades críticas en el equipo del usuario asistencial, el CVE relacionado y la solución indicada para mitigar una posible intrusión.

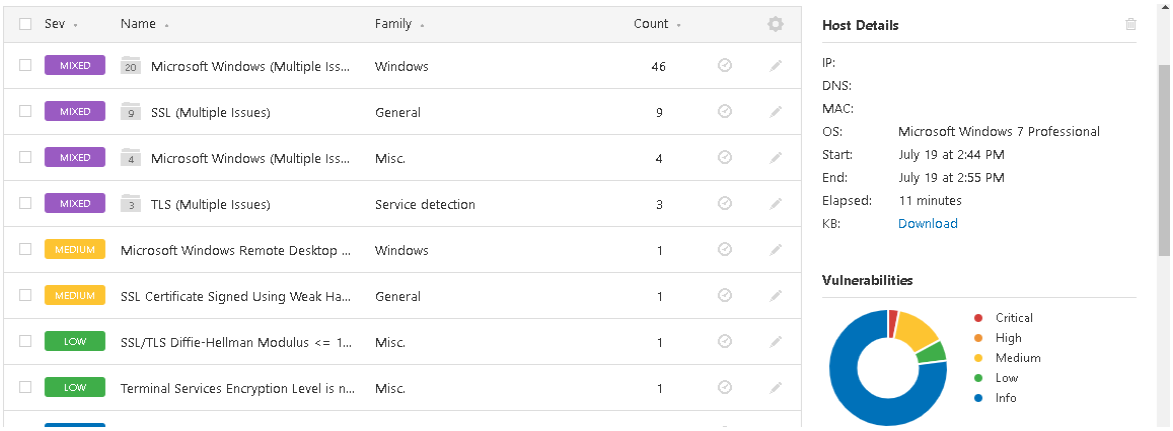
Ilustración 35. Resumen de vulnerabilidades críticas detectadas en el Equipo Usuario Asistencial



Fuente: elaboración propia

A continuación, se puede observar en la Figura 36 un resumen de las vulnerabilidades altas y medias en el equipo del usuario asistencial.

Ilustración 36. Resumen de vulnerabilidades altas y medias detectadas en el Equipo Usuario Asistencial



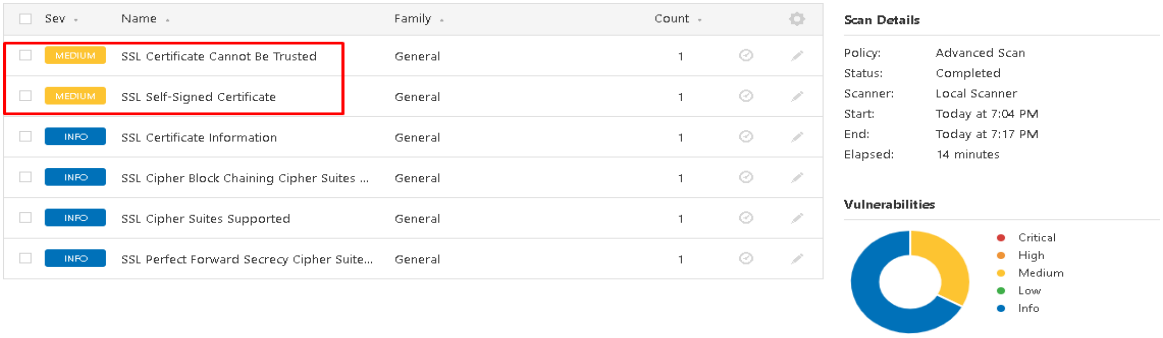
Fuente: elaboración propia

7.2.6 Firewall. A continuación, se puede observar en la Figura 37 una vulnerabilidad media en el firewall.

- **Vulnerabilidad de certificado autofirmado.**

El firewall maneja un certificado autofirmado (gratuito) que no es verificado por una entidad certificadora de confianza, permitiendo que la seguridad en la transmisión de la información se vea comprometida

Ilustración 37. Vulnerabilidad de certificado autofirmado



Fuente: elaboración propia

7.2.7 Servicios Publicados hacia Internet. A continuación, se puede observar en la Figura 38 una vulnerabilidad critica en los servicios expuestos a internet.

- **Vulnerabilidad de Versión del PHP.**

La versión del PHP que tiene instalada no cuenta con soporte, permitiendo a un atacante remoto ejecución de código malicioso.

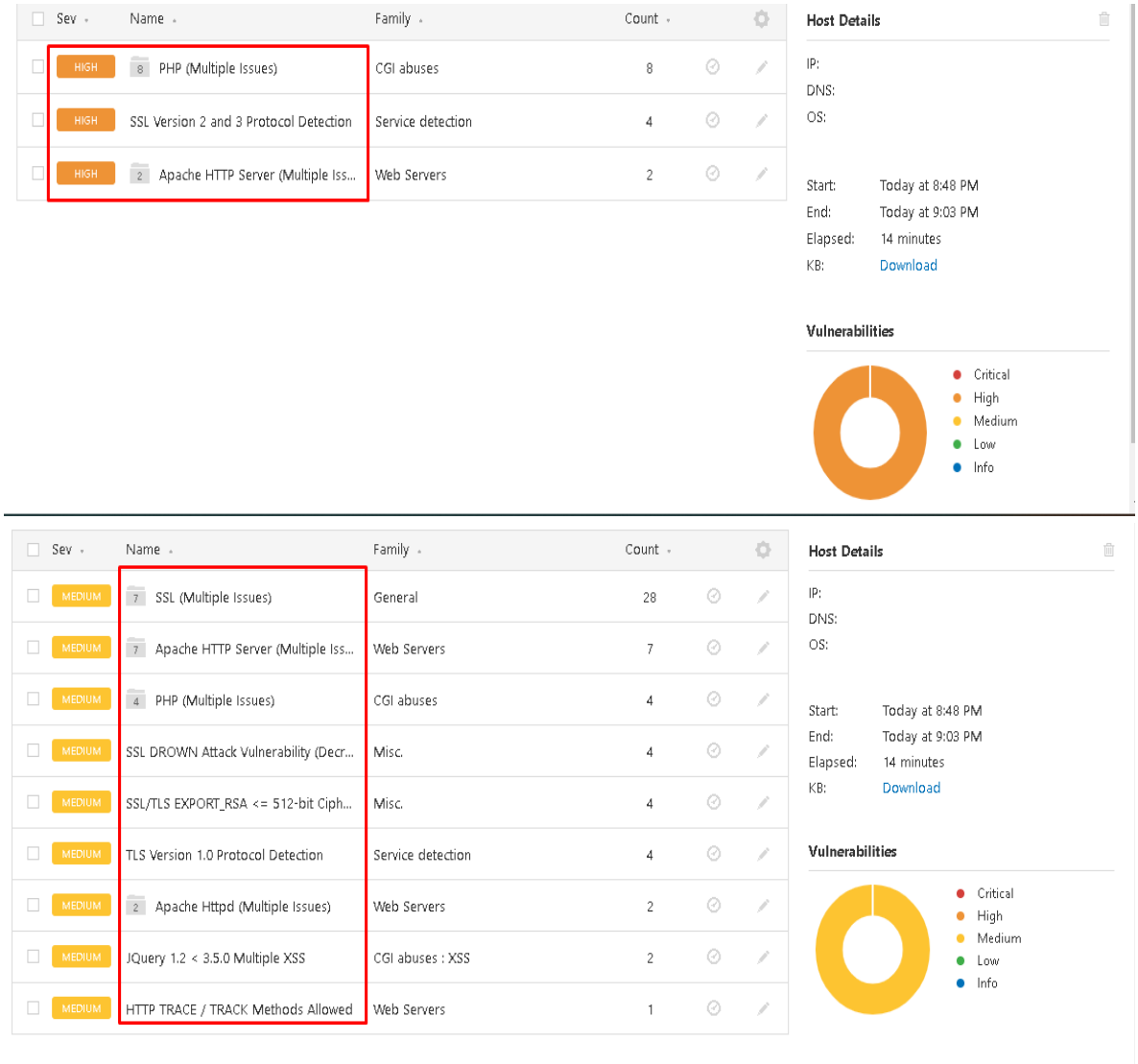
Ilustración 38. Vulnerabilidad de Versión del PHP

Fuente: elaboración propia

7.2.8 Resumen de vulnerabilidades detectadas en los Servicios Publicados hacia Internet.

A continuación, se puede observar en la Figura 39 un resumen de las vulnerabilidades detectadas en los servicios publicados hacia internet.

Ilustración 39. Resumen de vulnerabilidades detectadas en los Servicios Publicados hacia Internet



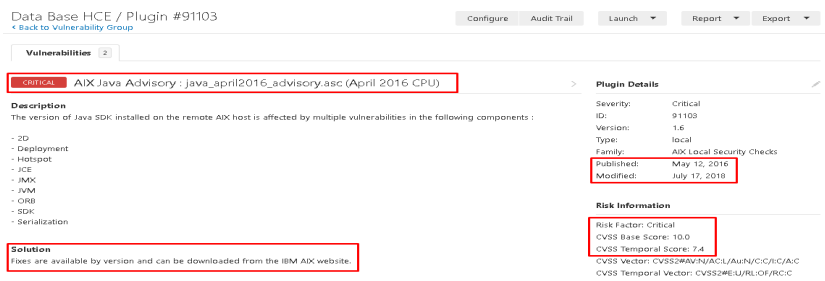
Fuente: elaboración propia

7.3 DESARROLLO DE OBJETVO 3: CLASIFICAR LAS VULNERABILIDADES ENCONTRADAS EN LA APLICACIÓN DE HISTORIA CLÍNICA ELECTRÓNICA.

Para el desarrollo del objetivo 3 se utiliza la cuarta fase de la metodología PTES donde se clasifican las vulnerabilidades antes encontradas en los diferentes dispositivos de red que hacen parte de la aplicación de Historia Clínica Electrónica como se puede observar en el Cuadro 3, se toma como base el impacto que puede generar a la Clínica si la vulnerabilidad es explotada y el reporte del CVE asociado en la página de INCIBE.[44] Las vulnerabilidades se clasifican por su nivel de impacto de la siguiente forma:

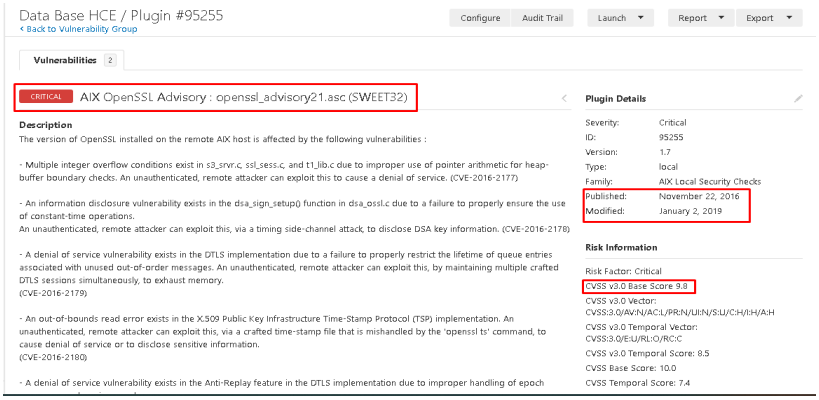
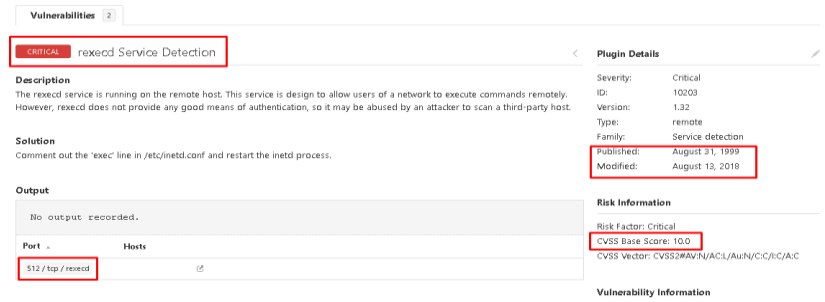
- **Vulnerabilidad Critica (Nivel de impacto Crítico):** La vulnerabilidad permite que la amenaza se propague sin que el usuario realice acciones.
- **Vulnerabilidad Alta (Nivel de impacto Alto):** Pone en riesgo la confidencialidad, integridad o disponibilidad de la información o de los recursos de procesamiento.
- **Vulnerabilidad Media (Nivel de impacto Medio):** No afecta a muchos usuarios y se puede combatir fácilmente con configuraciones, auditorias, entre otros. [45]

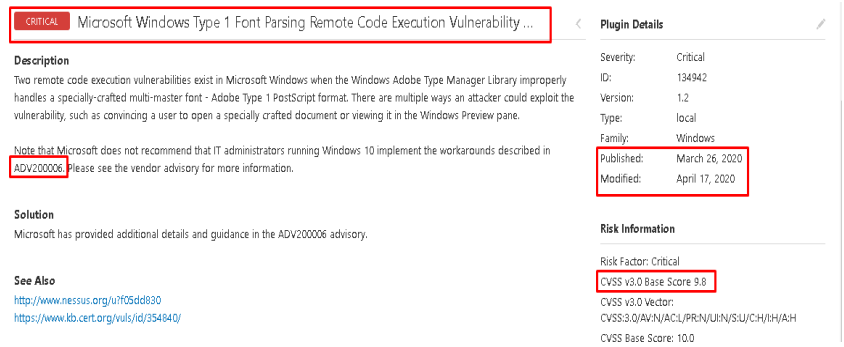
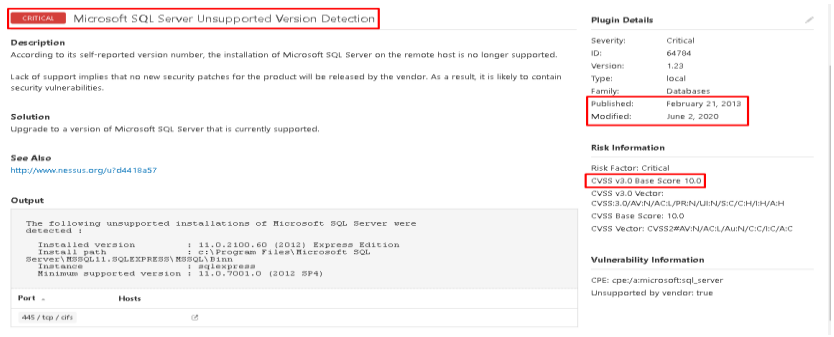
Cuadro 3. Nivel de criticidad de las vulnerabilidades

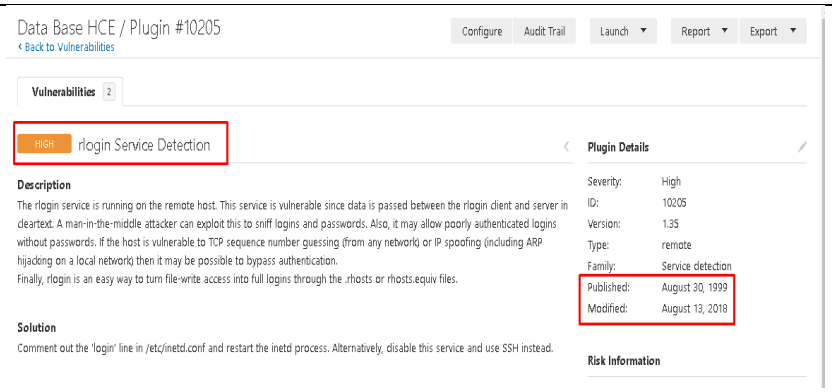
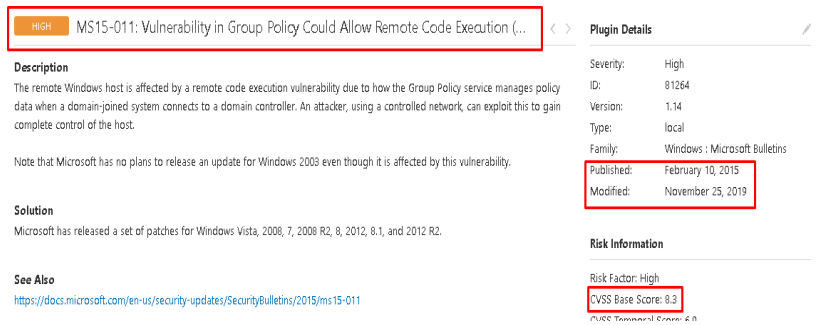
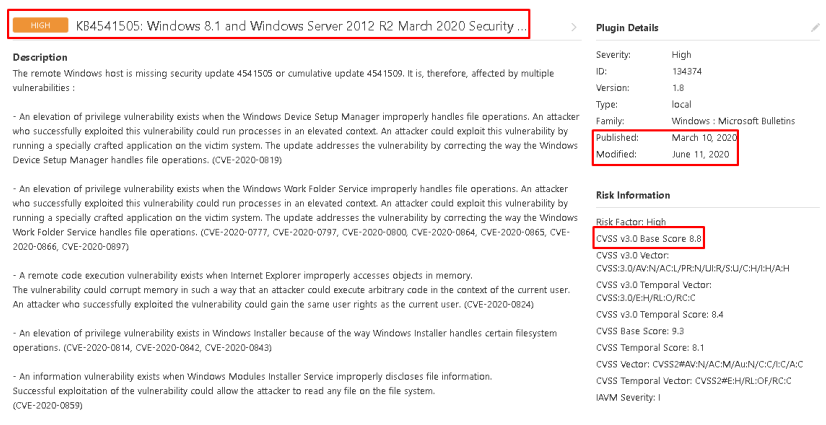
Vulnerabilidad	Criticidad	Evidencia Nessus
Vulnerabilidad de AIX Java en la base de datos.	Critica	**Ilustración 40.** Vulnerabilidad de AIX Java en la base de datos. 

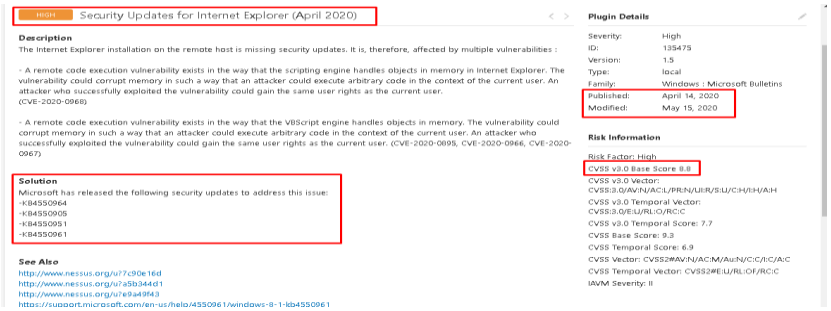
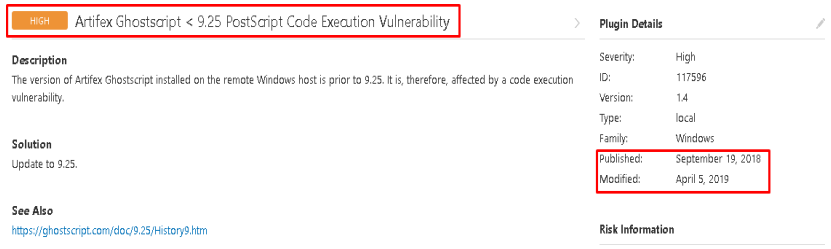
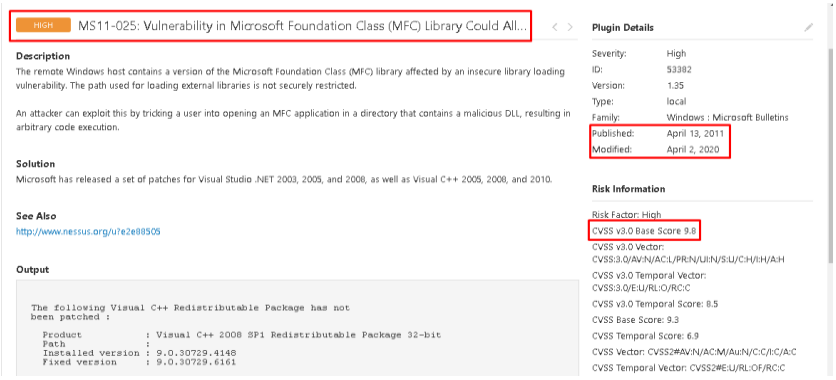
[44] INCIBE. Ciberseguridad CVE. [Sitio web]. Colombia: [Consulta: 10 de julio 2020]. Disponible en https://www.incibe.es/

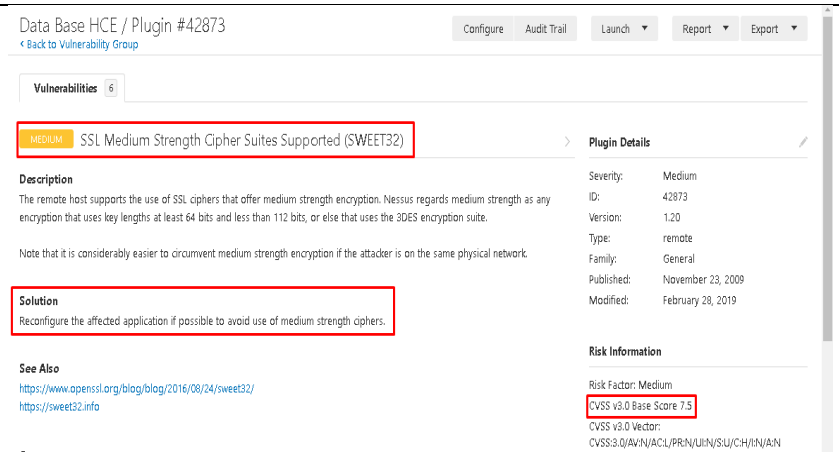
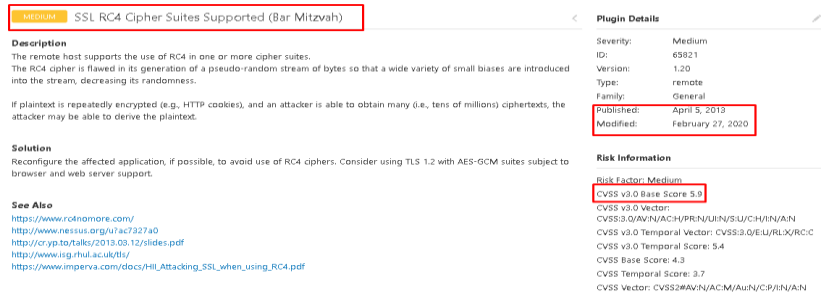
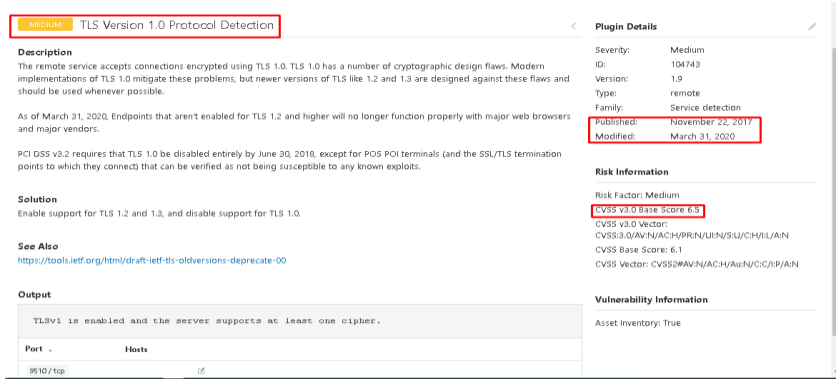
[45] TECNOLOGIA + INFORMATICA. Vulnerabilidades informáticas. [Sitio web]. Colombia: [Consulta: 30 de marzo 2020]. Disponible en https://www.tecnologia-informatica.com/vulnerabilidades-informaticas/

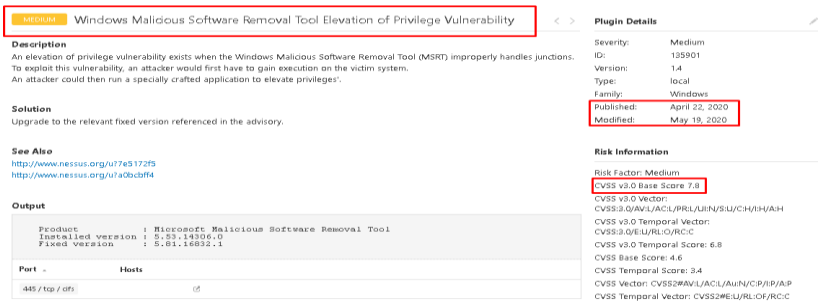
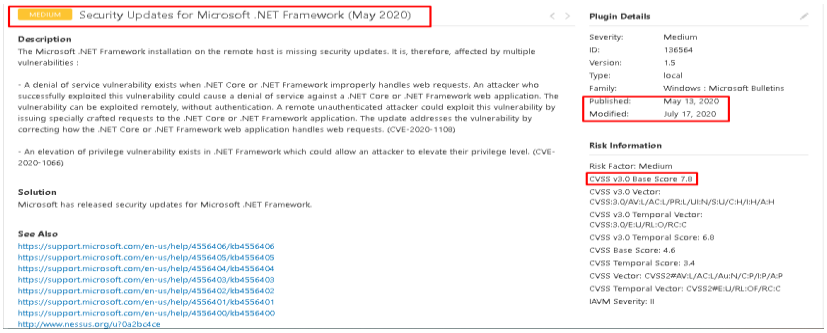
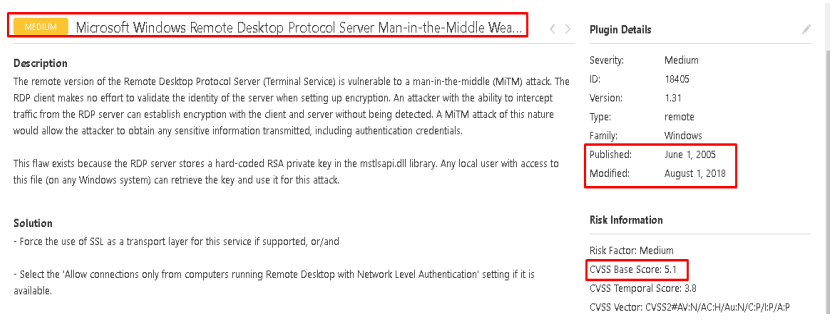
		Fuente: elaboración propia
Vulnerabilidad de AIX Open SSL en la base de datos.	Critica	**Ilustración 41.** Vulnerabilidad de AIX Open SSL en la base de datos.  Fuente: elaboración propia
Vulnerabilidad Rexecd Service en la base de datos.	Critica	**Ilustración 42.** Vulnerabilidad Rexecd Service en la base de datos.  Fuente: elaboración propia
Vulnerabilidad Antivirus Kaspersky en el servidor terminal server HCE.	Critica	**Ilustración 43.** Vulnerabilidad Antivirus Kaspersky en el servidor terminal server HCE.

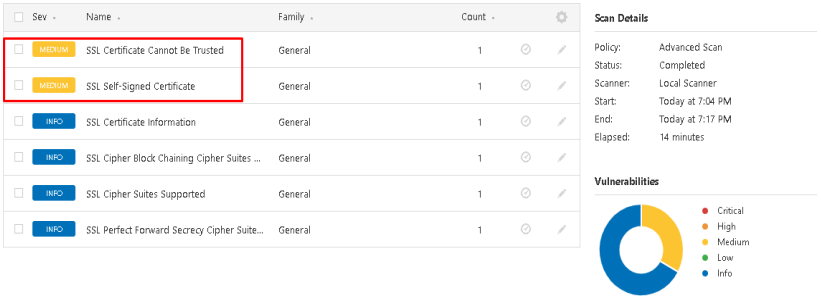
		 Fuente: elaboración propia
Vulnerabilidad Ejecución código remoto en el servidor terminal server HCE.	Critica	**Ilustración 44.** Vulnerabilidad Ejecución código remoto en el servidor terminal server HCE.  Fuente: elaboración propia
Vulnerabilidad Microsoft SQL Server en el servidor de aplicación HCE.	Critica	**Ilustración 45.** Vulnerabilidad Microsoft SQL Server en el servidor de aplicación HCE.  Fuente: elaboración propia
Vulnerabilidad rlogin Service en la base de datos.	Alta	**Ilustración 46.** Vulnerabilidad rlogin Service en la base de datos.

		 Fuente: elaboración propia
Vulnerabilidad de código remoto en el servidor terminal server HCE.	Alta	**Ilustración 47.** Vulnerabilidad de código remoto en el servidor terminal server HCE.  Fuente: elaboración propia
Vulnerabilidad de actualización acumulativa en el servidor terminal server HCE.	Alta	**Ilustración 48.** Vulnerabilidad de actualización acumulativa en el servidor terminal server HCE.  Fuente: elaboración propia
Vulnerabilidad actualización	Alta	**Ilustración 49.** Vulnerabilidad actualización de internet explorer en el servidor terminal server HCE.

de internet explorer en el servidor terminal server HCE.		 Fuente: elaboración propia
Vulnerabilidad de Artifex Ghostscript en el servidor terminal server HCE.	Alta	**Ilustración 50.** Vulnerabilidad de Artifex Ghostscript en el servidor terminal server HCE.  Fuente: elaboración propia
Vulnerabilidad MFC en el servidor terminal server HCE.	Alta	**Ilustración 51.** Vulnerabilidad MFC en el servidor terminal server HCE.  Fuente: elaboración propia
Vulnerabilidad Cipher Suites SSL en la base de datos.	Media	**Ilustración 52.** Vulnerabilidad Cipher Suites SSL en la base de datos.

		 Fuente: elaboración propia
Vulnerabilidad Cipher Suites SSL RC4 en la base de datos.	Media	**Ilustración 53.** Vulnerabilidad Cipher Suites SSL RC4 en la base de datos.  Fuente: elaboración propia
Vulnerabilidad TLS Versión 1.0 en la base de datos.	Media	**Ilustración 54.** Vulnerabilidad TLS Versión 1.0 en la base de datos.  Fuente: elaboración propia

Vulnerabilidad de elevación de permisos en el servidor terminal server HCE.	Media	**Ilustración 55.** Vulnerabilidad de elevación de permisos en el servidor terminal server HCE.  Fuente: elaboración propia
Vulnerabilidad de .Net Framework en el servidor terminal server HCE.	Media	**Ilustración 56.** Vulnerabilidad de .Net Framework en el servidor terminal server HCE.  Fuente: elaboración propia
Vulnerabilidad *Remote desktop Man in the middle* en el servidor de aplicación HCE.	Media	**Ilustración 57.** Vulnerabilidad *Remote desktop Man in the middle* en el servidor de aplicación HCE.  Fuente: elaboración propia

Vulnerabilidad de certificado autofirmado en el firewall.	Media	**Ilustración 58.** Vulnerabilidad de certificado autofirmado en el firewall.  Fuente: elaboración propia

Fuente: elaboración propia

7.4 DESARROLLO DEL OBJETIVO 4: DESCRIBIR LAS VULNERABILIDADES QUE IMPACTAN DE MANERA NEGATIVA A LA CLÍNICA

Para el desarrollo del objetivo 4 se utiliza la séptima fase de la metodología PTES que consiste en presentar el informe final listando las vulnerabilidades de acuerdo con su nivel de criticidad, los riesgos encontrados y las recomendaciones para mitigarlos.

7.4.1 Base de datos. A continuación, se describen cada una de las vulnerabilidades encontradas en la base de datos que impactan de manera negativa a la clínica y la solución para mitigar los riesgos.

- **Vulnerabilidad critica: AIX java CVE-2016-0376**

Descripción de la vulnerabilidad: La versión de Java SDK instalada en el host AIX remoto se ve afectada por múltiples vulnerabilidades en los siguientes componentes: 2D, *deployment*, *hospot*, JCE, SDK y serialización, permitiendo a un atacante remoto saltar las medidas de aseguramiento de un espacio e introducir código malicioso.[46]

Solución: Para corregir esta vulnerabilidad se debe ingresar al sitio web de IBM AIX y descargar la actualización de corrección según la versión utilizada.

- **Vulnerabilidad critica: AIX open SSL CVE-2016-2180**

Descripción de la vulnerabilidad: la versión de OPENSSL instalada en el *host* remoto AIX esta desactualizada, permitiendo a un atacante remoto un ataque de denegación de servicio por medio de un archivo corrupto llamado OPENSSL TS.[47]

Solución: Para corregir esta vulnerabilidad se debe descargar la actualización correspondiente desde el sitio web de IBM AIX.

- **Vulnerabilidad alta: Ejecución del servicio RLOGIN CVE-1999-0651**

[46] NIST. Base de datos nacional de vulnerabilidades. [Sitio web]. Colombia: [Consulta: 06 de noviembre 2020]. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2016-0376
[47] NIST. Base de datos nacional de vulnerabilidades. [Sitio web]. Colombia: [Consulta: 06 de noviembre 2020]. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2016-2180

Descripción de la vulnerabilidad: El servicio RLOGIN se está ejecutando en el servidor donde se encuentra la base de datos, este servicio es inseguro porque no tiene cifrado de los datos que se transmiten por la red y el método de autenticación es la dirección IP, permitiendo a un atacante remoto un ataque de Spoofing IP.[48]
Solución: Para corregir esta vulnerabilidad se debe implementar un protocolo de comunicación seguro como SSH.

- **Vulnerabilidad media: TLS Versión 1.0**

Descripción de la vulnerabilidad: El servicio remoto acepta conexiones cifradas con TLS 1.0. TLS 1.0 tiene una serie de defectos de diseño criptográfico. Las implementaciones modernas de TLS 1.0 mitigan estos problemas, pero las versiones más nuevas de TLS como 1.2 y 1.3 están diseñadas contra estas fallas y deben usarse siempre que sea posible. A partir del 31 de marzo de 2020, los terminales que no estén habilitados para TLS 1.2 y versiones posteriores ya no funcionarán correctamente con los principales navegadores web y los principales proveedores.

Solución: Para corregir esta vulnerabilidad se debe habilitar la compatibilidad con TLS 1.2 y 1.3 y deshabilitar la compatibilidad con TLS 1.0

7.4.2 Servidor terminal server. A continuación, se describen cada una de las vulnerabilidades encontradas en el servidor de terminal server que impactan de manera negativa a la clínica y la solución para mitigar los riesgos.

- **Vulnerabilidad critica: Antivirus Kaspersky**

Descripción de la vulnerabilidad: El antivirus Kaspersky que se encuentra instalado en el servidor no está ejecutando el motor o las firmas están desactualizadas, permitiendo que un atacante pueda ejecutar código malicioso e infectar los dispositivos de la red.

[48] NIST. Base de datos nacional de vulnerabilidades. [Sitio web]. Colombia: [Consulta: 06 de noviembre 2020]. Disponible en https://nvd.nist.gov/vuln/detail/CVE-1999-0651

Solución: Para corregir esta vulnerabilidad se debe revisar que la licencia y las firmas del antivirus kaspersky se encuentren activas y actualizadas y que todos los servicios se estén ejecutando correctamente.

- **Vulnerabilidad critica: Versión de SQL Server sin soporte**

Descripción de la vulnerabilidad: la versión SQL del servidor ya no cuenta con soporte eso implica que el proveedor no lanzará nuevos parches de seguridad para el producto, permitiendo que un atacante aproveche las vulnerabilidades existentes para explotarlas y atacarlas.

Solución: Para corregir esta vulnerabilidad se debe actualizar a una versión de Microsoft SQL Server que cuente con soporte por parte del proveedor.

- **Vulnerabilidad alta: Internet Explorer desactualizado CVE-2020-0968**

Descripción de la vulnerabilidad: La versión de internet Explorer se encuentra desactualizada y cuenta con vulnerabilidades, permitiendo que un atacante remoto aproveche las vulnerabilidades para ejecutar código malicioso en el motor de comando de los objetos de memoria del IE.[49]

Solución: Para corregir esta vulnerabilidad se deben instalar las siguientes actualizaciones: KB4550964, KB4550905, KB4550951 y KB4550961.

- **Vulnerabilidad alta: Visual Studio CVE-2010-3190**

Descripción de la vulnerabilidad: la ruta utilizada para cargar bibliotecas externas no está restringida de forma segura, permitiendo que un atacante aproveche esto y engañe a un usuario para que abra una aplicación MFC en un directorio que contiene un dll malicioso ejecutando código arbitrario.[50]

[49] NIST. Base de datos nacional de vulnerabilidades. [Sitio web]. Colombia: [Consulta: 06 de noviembre 2020]. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2020-0968
[50] NIST. Base de datos nacional de vulnerabilidades. [Sitio web]. Colombia: [Consulta: 06 de noviembre 2020]. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2010-3190

Solución: Para corregir esta vulnerabilidad Microsoft ha lanzado un conjunto de parches para Visual Studio .NET 2003, 20055 y 2008, así como para visual C++ 2005, 2008 y 2010.

7.4.3 Equipo Cliente Asistencial y Administrativo. A continuación, se describen cada una de las vulnerabilidades encontradas en los equipos cliente asistencial y administrativo que impactan de manera negativa a la clínica y la solución para mitigar los riesgos.

- **Vulnerabilidad critica: Versión de Windows sin soporte**

Descripción de la vulnerabilidad: la versión del sistema operativo (Windows 7) del servidor ya no cuenta con soporte por parte de Microsoft eso implica que el proveedor no lanzará nuevos parches de seguridad para el producto, permitiendo que un atacante aproveche las vulnerabilidades existentes para explotarlas y atacarlas.
Solución: Para corregir esta vulnerabilidad se debe actualizar el sistema operativo a una versión que sea soportada por Microsoft (Windows 10 en adelante).

Adicional a las vulnerabilidades mencionadas anteriormente encontradas por medio de la herramienta de Pentesting NESSUS, se detectan por medio del levantamiento de información las siguientes vulnerabilidades que impactan de manera negativa a la Clínica:

- **La versión del Firewall Fortigate cuenta en la actualidad con una versión de FortiOS 5.6.9. Al validar las posibles vulnerabilidades para este tipo de versión se identifica el CVE-2018-13383 de criticidad Alta.**

Descripción de la vulnerabilidad: Una vulnerabilidad de desbordamiento de buffer de almacenamiento dinámico en el portal web FortiOS SSL VPN puede provocar la finalización del servicio web para los usuarios registrados o la posible ejecución remota de código en FortiOS. Esto sucede cuando un usuario autenticado visita una página web específicamente diseñada dando paso a una falla en el manejo adecuado de los datos href de JavaScript que son intermediados por un servidor proxy. Esto solo afecta al “modo web” SSL VPN (el modo túnel SSL VPN no se ve

afectado), dando bases para un ataque de Denegación de Servicio ejecutado por código remoto. [51]

Solución: Para corregir esta vulnerabilidad se debe actualizar la versión de FortiOS por la que el fabricante sugiera estable y cuente con todos los parches de seguridad actuales.

- **La Clínica no cuenta con una política de contraseñas seguras para HCE, y para el acceso a la aplicación a través del servidor de terminal server.**

Descripción de la vulnerabilidad: Los posibles ataques en los que se pueden ver comprometidas las credenciales de los usuarios son:
Ataques de Diccionario, que consisten en intentar autenticarse de forma continua a los sistemas, tomando posibles contraseñas de una base de datos creada.
Ataques de Fuerza Bruta, utiliza la misma metodología de un ataque de diccionario, con la diferencia que este se genera dependiendo de la cantidad de posibles combinaciones.

Solución: Para corregir esta vulnerabilidad se debe implementar dentro del área de TI políticas de contraseñas seguras para cada una de las conexiones, algunas sugerencias son: mayúsculas, minúsculas, números, caracteres especiales y una longitud considerable. Estas políticas deben ser de conocimiento y de carácter obligatorio para todo el personal de la clínica.

- **Algunas estaciones de trabajo no tienen aplicadas los KB descargadas debido a que estos equipos no se reinician constantemente.**

Descripción de la vulnerabilidad: Al no aplicarse de forma pertinente los KB de actualización en las máquinas de trabajo, hace que una vulnerabilidad esté activa en el tiempo y pueda ser explotada.

Solución: Para corregir esta vulnerabilidad se debe concientizar a todo el personal de la clínica en reiniciar al menos una vez a la semana los computadores para

[51] NIST. Base de datos nacional de vulnerabilidades. [Sitio web]. Colombia: [Consulta: 06 de noviembre 2020]. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2018-13383

aplicar las actualizaciones descargadas, en caso de no ser posible reiniciar cuando las actualizaciones muestren el aviso de instalación.

- **Los servidores que están expuestos a internet se encuentran en la misma VLAN de los servidores internos (Bases de datos, historia clínica electrónica, aplicaciones, servidor de archivos, entre otros).**

Descripción de la vulnerabilidad: A través de vulnerabilidades que puedan presentar estos servidores expuestos a internet, se pueden producir ataques de código remoto afectando a todos los servidores que están en la misma VLAN, debido a que no existe una barrera (Firewall) que impida el acceso a otros servidores no autorizados.

Solución: Para corregir esta vulnerabilidad se debe segmentar de la red (VLANS), que separen los servidores que manejan información sensible de la red en general.

- **La clínica no maneja guías de *hardening* para el alistamiento de dispositivos nuevos en la red.**

Descripción de la vulnerabilidad: Al no existir guías de *hardening* para el alistamiento de los dispositivos, no es posible asegurar que se cumplan buenas prácticas como deshabilitar protocolos inseguros, inhabilitar servicios que no se utilizan, eliminar usuarios y contraseñas por defecto, entre otros, estas provocan vulnerabilidades que pueden convertirse en ataques fácilmente.

Solución: Para corregir esta vulnerabilidad se deben implementar guías de *hardening* y ser socializadas al equipo de trabajo de TI o a quien pueda interesar.

- **El usuario y la contraseña es la misma para la conexión de la base de datos (ODBC), adicional la información de esta configuración no se encuentra cifrada.**

Descripción de la vulnerabilidad: Esta vulnerabilidad es crítica porque un atacante puede obtener por medio de un *sniffer* (Wireshark), los datos de la conexión ODBC que viajan en texto plano desde el servidor terminal hacia la base de datos cada vez que se realiza un *login* a la aplicación de historia clínica electrónica y con estos

datos de conexión puede acceder al servidor al servidor donde se encuentra almacenada la base de datos.

Solución: Para corregir esta vulnerabilidad se debe implementar dentro del área de TI políticas de contraseñas seguras para la conexión a la base de datos, algunas sugerencias son: mayúsculas, minúsculas, números, caracteres especiales y una longitud considerable. Estas políticas deben ser de conocimiento y de carácter obligatorio para todo el personal de TI o que tiene acceso a la base de datos. Adicional implementar un protocolo de comunicación cifrado para que estas credenciales no se visualicen en texto plano.

- **Préstamo de usuarios para el ingreso a la aplicación de Historia Clínica Electrónica entre los empleados.**

Descripción de la vulnerabilidad: Esta mala práctica coloca en riesgo la confidencialidad e integridad de la información, debido a que no se puede tener un control verídico en cuanto a consulta, modificación o eliminación de datos sensibles y confidenciales. Un atacante puede recurrir a ataques de ingeniería social y realizar modificación o eliminación en la información sin ser detectado.
Solución: Para corregir esta vulnerabilidad se debe concientizar a todo el personal de la clínica en los riesgos que conlleva esta mala práctica, todos los ataques a los que puede estar expuesto los dispositivos de red y la confidencialidad, integridad y disponibilidad de la información.

8. CONCLUSIONES

Se puede concluir de acuerdo con lo analizado con la herramienta NESSUS que en la clínica existen vulnerabilidades críticas, altas y medias que colocan en riesgo la disponibilidad, integridad y confidencialidad de la información en su transmisión por los diferentes dispositivos de la red, lo que sugiere gran impacto en el negocio en caso de ser explotada por un atacante.

Por medio de las vulnerabilidades encontradas en la clínica se logró realizar un análisis profundo y categorizar la amenaza de acuerdo con su criticidad e impacto.

Se observa por medio de la recolección de la información el desconocimiento de procesos como políticas de contraseñas seguras, guías de *Harding*, segmentación de la red, políticas de reinicio de los dispositivos para aplicar actualizaciones por parte del personal de TI y empleados de la clínica.

Se evidencia con base a las vulnerabilidades encontradas en la clínica que pueden ser explotadas por medio de ataques como intrusión y ejecución de código malicioso, denegación de servicios, *Spoofing* IP e ingeniería social.

Se determino por medio de la herramienta NESSUS y la fase de levantamiento de información sobre la metodología PTES que cada una de las vulnerabilidades encontradas es un vector de ataque y es posible que otorgue acceso a un atacante a los diferentes dispositivos de red, información, servicios y procesos sensibles de la clínica.

9. RECOMENDACIONES

Se recomienda corregir la vulnerabilidad CVE-2016-0376 relacionada con el AIX Java en la base de datos, la solución consiste en ingresar al sitio web de IBM AIX y descargar la actualización de corrección según la versión utilizada.

Se recomienda corregir la vulnerabilidad CVE-2016-2180 relacionada con el AIX SSL en la base de datos, la solución consiste en se debe descargar la actualización correspondiente desde el sitio web de IBM AIX.

Se recomienda corregir la vulnerabilidad CVE-1999-0651 relacionada con la ejecución del servicio RLOGIN en la base de datos, la solución consiste en implementar un protocolo de comunicación seguro como SSH.

Se recomienda corregir la vulnerabilidad relacionada con la versión TLS 1.0, la solución consiste en habilitar la compatibilidad con TLS 1.2 y 1.3 y deshabilitar la compatibilidad con TLS 1.0

Se recomienda corregir la vulnerabilidad relacionada con el Antivirus Kaspersky, la solución consiste en revisar que la licencia y las firmas del antivirus kaspersky se encuentren activas y actualizadas y que todos los servicios se estén ejecutando correctamente.

Se recomienda corregir la vulnerabilidad relacionada con la versión del SQL Server, la solución consiste en actualizar a una versión de Microsoft SQL Server que cuente con soporte por parte del proveedor.

Se recomienda corregir la vulnerabilidad CVE-2020-0968 relacionada con la versión del Internet Explorer, la solución consiste en instalar las siguientes actualizaciones: KB4550964, KB4550905, KB4550951 y KB4550961.

Se recomienda corregir la vulnerabilidad CVE-2010-3190 relacionada con Visual Studio, la solución consiste en instalar un conjunto de parches para Visual Studio .NET 2003, 20055 y 2008, así como para visual C++ 2005, 2008 y 2010 que lanzo Microsoft.

Se recomienda corregir la vulnerabilidad relacionada con Windows 7, la solución consiste en actualizar el sistema operativo a una versión que sea soportada por Microsoft (Windows 10 en adelante).

Se recomienda corregir la vulnerabilidad CVE-2018-13383 relacionada con la versión del Firewall Fortigate, la solución consiste en actualizar la versión de FortiOS por la que el fabricante sugiera estable y cuente con todos los parches de seguridad actuales.

Se recomienda implementar dentro del área de TI políticas de contraseñas seguras para cada una de las conexiones, algunas sugerencias son: mayúsculas, minúsculas, números, caracteres especiales y una longitud considerable. Estas políticas deben ser de conocimiento y de carácter obligatorio para todo el personal de la clínica.

Se recomienda concientizar a todo el personal de la clínica en reiniciar al menos una vez a la semana los computadores para aplicar las actualizaciones descargadas, en caso de no ser posible reiniciar cuando las actualizaciones muestren el aviso de instalación.

Se recomienda segmentar de la red (VLANS), que separen los servidores que manejan información sensible de la red en general.

Se recomienda implementar guías de *hardening* y ser socializadas al equipo de trabajo de TI o a quien pueda interesar.

Se recomienda implementar dentro del área de TI políticas de contraseñas seguras para la conexión a la base de datos, algunas sugerencias son: mayúsculas, minúsculas, números, caracteres especiales y una longitud considerable. Estas políticas deben ser de conocimiento y de carácter obligatorio para todo el personal de TI o que tiene acceso a la base de datos. Adicional implementar un protocolo de comunicación cifrado para que estas credenciales no se visualicen en texto plano.

Se recomienda concientizar a todo el personal de la clínica en los riesgos que conlleva esta mala práctica, todos los ataques a los que puede estar expuesto los dispositivos de red y la confidencialidad, integridad y disponibilidad de la información.

BIBLIOGRAFÍA

ABC SOFTWARE. Alonso, Rodrigo. Los riesgos de un ciberataque a los hospitales durante la pandemia de coronavirus. Republica checa. Disponible en: https://www.abc.es/tecnologia/informatica/software/abci-riesgos-ciberataque-hospitales-durante-pandemia-coronavirus-202003190858_noticia.html

BLOGSPOT. Metodología PTES (Penetration Testing Execution Standard). Disponible en http://blogdeauditoriadeseguridad.blogspot.com/2017/09/metodologia-ptes-penetration-testing.html

CATOIRA, FABIO. Funcionalidades de monitoreo continuo de Nessus. Disponible en www.welivesecurity.com/la-es/2017/10/27/reglas-de-yara-nessus

CCIT.ORG. Informe de las tendencias del cibercrimen en Colombia (2019-2020). Disponible en https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

CONSTITUCIÓN POLITICA DE COLOMBIA. Artículo 15. Disponible en https://www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-15#:~:text=fundamentales%20%2F%20Art%C3%ADculo%2015-,Art%C3%ADculo%2015,debe%20respetarlos%20y%20hacerlos%20respetar

CYBERSECURE. FORTINET informa vulnerabilidades detectadas en sus productos. Disponible en https://portal.cci-entel.cl/Threat_Intelligence/Boletines/361/

DINERO. En solo tres meses Colombia sufrió 42 billones de intentos de ataques cibernéticos. Disponible en: https://www.dinero.com/actualidad/articulo/cuantos-ataques-ciberneticos-recibe-colombia/276556

EL PAIS ESPAÑA. La policía detecta un ciberataque al sistema informático de los hospitales. Disponible en: https://elpais.com/espana/2020-03-23/la-policia-detecta-un-ataque-masivo-al-sistema-informatico-de-los-hospitales.html

EL TIEMPO. Colombia sufrió 42 billones de intentos de ciberataques en 3 meses. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/colombia-sufrio-42-billones-de-intentos-de-ciberataques-en-3-meses-413666

FUNCIÓN PUBLICA. Ley 1266 de 2008. Disponible en https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

GLOBATIKA LAB. Metodología OSSTMM. Disponible en https://peritosinformaticos.es/metodologia-osstmm/

INCIBE. Ciberseguridad CVE. Disponible en https://www.incibe.es/

INSECUREDATA. Metodología de test de intrusión ISSAF. Disponible en http://insecuredata.blogspot.com/2009/04/metodologia-de-test-de-intrusion-issaf.html#:~:text=La%20metodolog%C3%ADa%20de%20test%20de,Planificaci%C3%B3n%20y%20Preparaci%C3%B3n

ISO. Norma ISO 27002:2013. Disponible en https://www.efectus.cl/wp-content/uploads/2018/12/Controles_ISO27002-2013.pdf

LAGOS, EDWIN. Análisis de vulnerabilidades y pruebas de penetración a la infraestructura tecnológica de empresa. Disponible en http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/15381/Informe.pdf?sequence=1

--------. Wireshark. [Sitio web]. Colombia: [Consulta: 30 de marzo 2020]. Disponible en https://www.ecured.cu/Wireshark

MEDIUM. ¿Qué es el pentesting?. Disponible en https://medium.com/@rootsec/pentesting-introducci%C3%B3n-cb40a8ae67ba

--------. Pentesting. Disponible en https://medium.com/@rootsec/pentesting-introducci%C3%B3n-cb40a8ae67ba

MINTIC. Ley 1273 de 2009. Disponible en https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

MUNDO HACKERS. Nessus. Disponible en https://mundo-hackers.weebly.com/nessus.html

NIST. CVE-2018-13383 Detail. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2018-13383

NIST. Base de datos nacional de vulnerabilidades. [Sitio web]. Colombia: [Consulta: 06 de noviembre 2020]. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2016-0264

NIST. Base de datos nacional de vulnerabilidades. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2016-2177

--------. -. Disponible en https://nvd.nist.gov/vuln/detail/CVE-1999-0618

--------. --------. Disponible en https://nvd.nist.gov/vuln/detail/CVE-1999-0651

--------. --------. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2016-2183

--------. --------. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2015-2808

--------. --------. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2015-0008

--------. --------. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2020-0968

--------. --------. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2020-0733

--------. --------. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2020-1108

--------. -------. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2018-16802

--------. --------. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2010-3190

--------. --------. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2005-1794

--------. --------. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2016-0376

--------. --------. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2016-2180

--------. --------. Disponible en https://nvd.nist.gov/vuln/detail/CVE-1999-0651

--------. --------. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2020-0968

--------. --------. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2010-3190

--------. --------. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2018-13383

PEREZ, IVAN. Maltego, la herramienta que te muestra qué tan expuesto estás en Internet. Disponible en https://www.welivesecurity.com/la-es/2014/02/19/maltego-herramienta-muestra-tan-expuesto-estas-internet/

REYES, ALONSO. Metodología de Pruebas OWASP. Disponible en http://www.reydes.com/d/?q=Metodologia_de_Pruebas_OWASP

SUIN JURISCOL. Ley 1581 de 2012. Disponible en http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1684507

TECNOLOGIA + INFORMATICA. Tipos de vulnerabilidades en informática. Disponible en https://www.tecnologia-informatica.com/vulnerabilidades-informaticas/

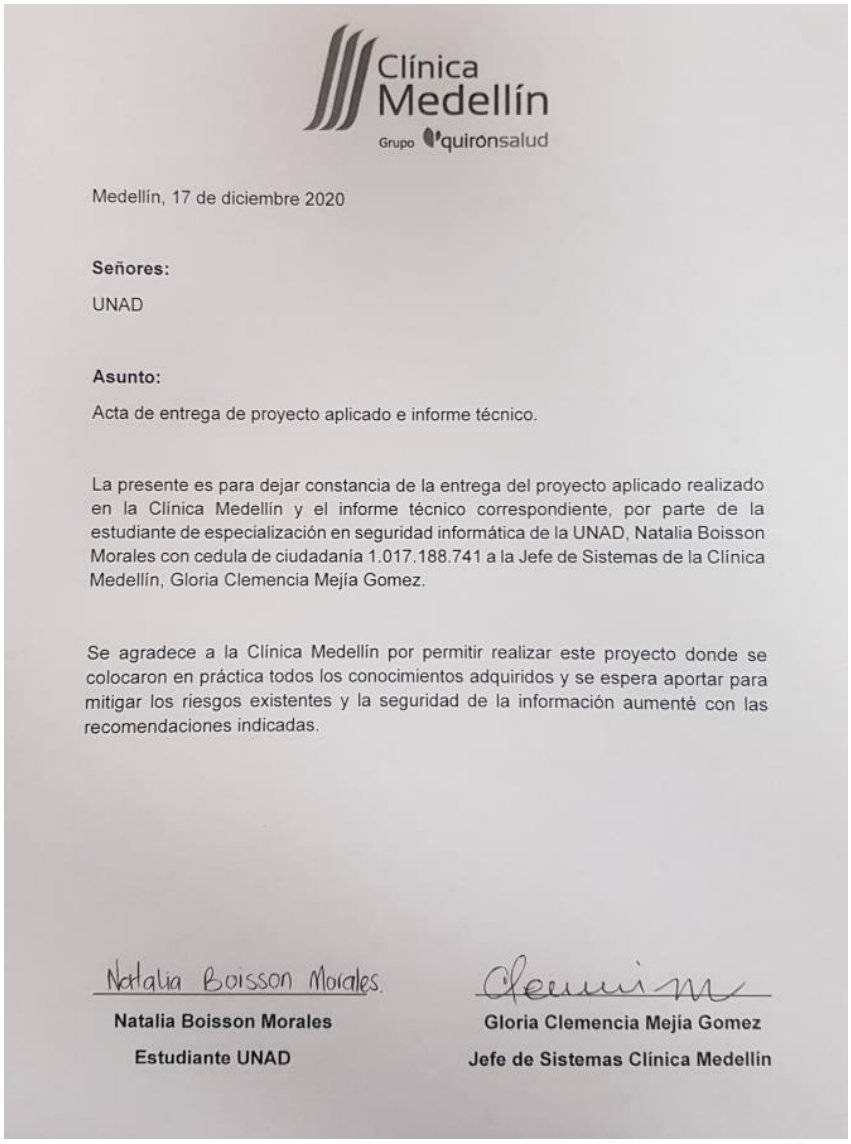
TECNOLOGIA + INFORMATICA. Vulnerabilidades informáticas. Disponible en https://www.tecnologia-informatica.com/vulnerabilidades-informaticas/

WELIVESECURITY. Datos personales de más de 2 millones de pacientes expuestos en Internet. Disponible en: https://www.welivesecurity.com/la-es/2018/08/07/datos-personales-pacientes-mexico-expuestos-internet/

ANEXOS

Entrega del proyecto e informe técnico a la Jefe de Sistemas de la Clínica Medellín

Ilustración 59. Entrega del proyecto e informe técnico a la Jefe de Sistemas de la Clínica Medellín



Clínica Medellín
Grupo quirónsalud

Medellín, 17 de diciembre 2020

Señores:

UNAD

Asunto:

Acta de entrega de proyecto aplicado e informe técnico.

La presente es para dejar constancia de la entrega del proyecto aplicado realizado en la Clínica Medellín y el informe técnico correspondiente, por parte de la estudiante de especialización en seguridad informática de la UNAD, Natalia Boisson Morales con cedula de ciudadanía 1.017.188.741 a la Jefe de Sistemas de la Clínica Medellín, Gloria Clemencia Mejía Gomez.

Se agradece a la Clínica Medellín por permitir realizar este proyecto donde se colocaron en práctica todos los conocimientos adquiridos y se espera aportar para mitigar los riesgos existentes y la seguridad de la información aumenté con las recomendaciones indicadas.

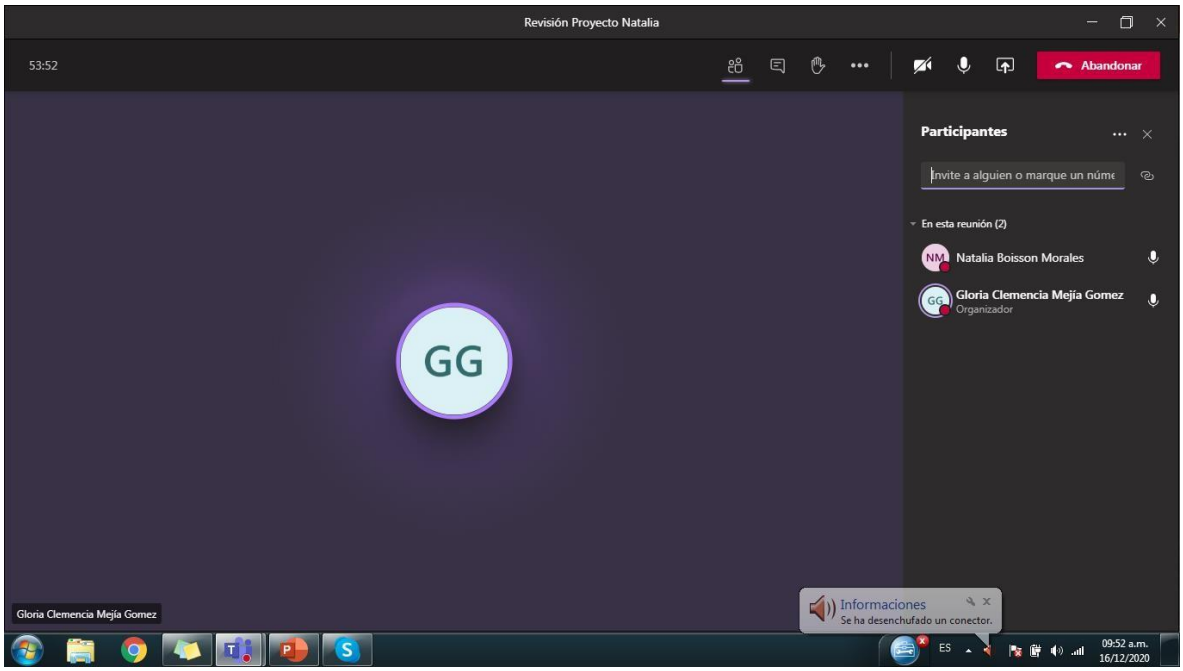
Natalia Boisson Morales.

Natalia Boisson Morales
Estudiante UNAD

Gloria Clemencia Mejía Gomez
Jefe de Sistemas Clínica Medellín

Fuente: elaboración propia.

Ilustración 60. Acta de entrega del proyecto e informe técnico a la Jefe de Sistemas de la Clínica Medellín



Fuente: elaboración propia.