UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE INF/TI

EXAMEN COMPLEXIVO

Componente Práctico, previo a la obtención del Título de:

INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

"Análisis de amenazas y vulnerabilidades informáticas basado en la Norma ISO 27002, en el proceso de citas del servidor web de una Institución"

AUTOR

Richard Manuel Catuto Pilay

LA LIBERTAD – ECUADOR

2021

APROBACIÒN DEL TUTOR

En mi calidad de tutor/tutora del trabajo de componente práctico del examen de carácter complexivo: "**Análisis de amenazas y vulnerabilidades informáticas basado en la Norma ISO 27002, en el proceso de citas del servidor web de una Institución**", elaborado por el sr. Catuto Pilay Richard Manuel, de la carrera de Tecnología de la Información de la Universidad Estatal Península de Santa Elena, me permito declarar que luego de haber orientado, estudiado y revisado, la apruebo en todas sus partes.

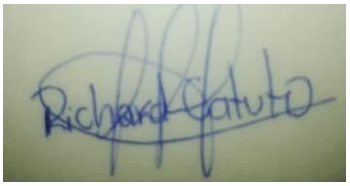
La libertad, marzo de 2021**.**

_____

Lsi. Daniel Quirumbay Yagual

DECLARACIÓN

El contenido del presente componente práctico del examen de carácter complexivo es de mi responsabilidad; el patrimonio intelectual del mismo pertenece a la Universidad Estatal Península de Santa Elena



Richard Manuel Catuto Pilay

AGRADECIMIENTO

Expresos mis agradecimientos a los directivos de la Clínica Santa Martha, que me autorizó para recolectar la información necesaria en mi proyecto de titulación.
A mi familia, que ha sido un apoyo incondicional para poder terminar esta etapa universitaria. A mi prima Paola Pozo que siempre me apoyo, me aconsejo a seguir luchando por mis objetivos.
A la Organización Plan Internacional, por su apoyo en mi etapa de universidad y las capacitaciones brindadas.
A los docentes de la UPSE por sus enseñanzas en los años de estudios. Y a mi tutor Daniel Quirumbay por la guía en mi proyecto de titulación.

Richard Manuel Catuto Pilay

DEDICATORIA

Dedico este trabajo a mis padres, por su apoyo y siempre creyeron en mi para culminar mis estudios.

A mis abuelitos que estarían felices por este logro, a mi hermano por su apoyo sin importar la distancia.

A mi ahijado que me inspira a ser una mejor persona y siga mis pasos.

A mi familia que me han dado fuerzas, respaldo para culminar esta bonita etapa de la vida.

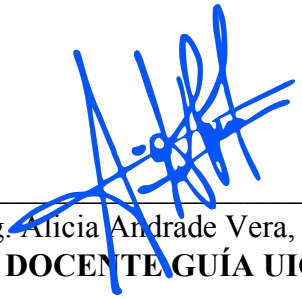
Richard Manuel Catuto Pilay

TRIBUNAL DE GRADO

Ing. Samuel Bustos Gaibor, Mgt.
DIRECTOR DE LA CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Ing. Iván Coronel Suárez, MSIA.
DOCENTE ESPECIALISTA

Lsi. Daniel Quirumbay Yagual, MSIA.
DOCENTE TUTOR



Ing. Alicia Andrade Vera, Mgt.
DOCENTE GUÍA UIC

RESUMEN

Este presente trabajo fue basado en detectar amenazas, vulnerabilidades, que se encuentran en los activos de información, ya que la clínica no cuenta con un control de seguridad informática antes ataques de cibernéticos, y esto puede generar perdida de información importante como historias clínicas, citas, tratamiento por paciente. Se propone elaborar un plan de seguridad informático alineado con los controles de normativa ISO 27002, para conocer el estado organizacional respecto a la seguridad informática, nos apoyamos en la herramienta informática Kali Linux con herramientas de análisis de vulnerabilidades NMAP, NIKTO, OWASP y aplicamos el estándar ISO para el control de posibles riesgos.

Se basa en llevar una auditoria donde a partir del análisis, escaneo de información se conocerá amenazas, los riegos por categorías sean estos altos, medios y bajos. La metodología de evaluación de seguridad del sistema de información ISSAF establece 3 fases importantes como: Planificación y Preparación (Organización), Evaluación y reportes (vulnerabilidades y posibles soluciones), para el control de la seguridad dentro de la clínica, especificando los roles por fases que nos llevaran a conocer los activos, procesos, todo el funcionamiento de la clínica para la reducción de incidentes de seguridad.

Con los resultados de los riesgos existentes y de los activos que se involucran antes las pérdidas de información, se espera minimizar los riesgos empleando controles de seguridad de la norma ISO 27002 lo cual ayuda a fortalecer tres aspectos importantes: la confidencialidad, integridad y disponibilidad de la información que corresponda a las necesidades de seguridad informática, de esta forma tendremos una protección de los datos, una vez aplicada políticas de seguridad informática mejorando los niveles de seguridad de la información de los procesos de la clínica.

ABSTRACT

This present work was based on detecting threats, vulnerabilities, found in information assets, since the clinic does not have a computer security control before cyber attacks, and this can generate loss of important information such as medical records, appointments, treatment per patient. It is proposed to develop a computer security plan aligned with the controls of ISO 27002 regulations, to know the organizational status regarding computer security, we rely on the Kali Linux computer tool with NMAP, NIKTO, OWASP vulnerability analysis tools and apply the ISO standard for the control of possible risks.

It is based on carrying out an audit where, from the analysis, information scanning, threats will be known, the risks by categories are high, medium and low. The ISSAF information system security evaluation methodology establishes 3 important phases such as: Planning and Preparation (Organization), Evaluation and reports (vulnerabilities and possible solutions), for the control of security within the clinic, specifying the roles by phases that will take us to know the assets, processes, all the operation of the clinic for the reduction of security incidents.

With the results of the existing risks and of the assets that are involved before the loss of information, it is expected to minimize the risks by employing security controls of the ISO 27002 standard which helps to strengthen three important aspects: confidentiality, integrity and availability of the information that corresponds to the computer security needs, in this way we will have data protection, once computer security policies have been applied, improving the information security levels of the clinic's processes.

Contenido

INDICE DE FIGURAS

INDICE DE TABLA

INDICE DE ANEXOS

Análisis de amenazas y vulnerabilidades informáticas basado en la Norma ISO 27002, en el proceso de citas del servidor web de una Institución

CAPÍTULO I

1. FUNDAMENTACIÓN

1.1 ANTECEDENTES

En la época actual las empresas son más competitivas debido a que manejan grandes cantidades de información, almacenan información, actividades y datos personales de sus clientes, todo esto como operación del negocio, por lo cual se convierte en un riesgo la exposición de dicha información y la mala manipulación de la misma, por lo tanto, es necesario establecer políticas, estándares necesarios que regulen de alguna manera la seguridad de esta [1].

Para proteger los sistemas de información de los crecientes niveles de amenazas cibernéticas, las organizaciones actualmente tienen la necesidad y hasta obligación de establecer programas o proyectos de seguridad informática y, debido a que las políticas de seguridad de la información son una base necesaria de los programas de seguridad organizacional, existe una necesidad de contribuciones académicas en esta importante área [2].

Por los riesgos que surgen las organizaciones en la administración de datos y posteriormente en su actividad, es importante ejecutar un análisis de amenazas basados en la normatividad ISO27002 para planificar los mejores procedimientos para neutralizar las amenazas que puedan abusar de las debilidades que pueda tener la institución privada. Actualmente la institución privada Clínica Santa Martha en la ciudad de La Libertad, requiere de una exploración de riesgos para tener una mirada más amplia con respecto a su estado de seguridad de datos y posteriormente proponer un tratamiento suficiente para disminuir los riesgos a niveles dignos para la organización, estableciendo políticas y normas que ayuden a limitar el efecto que puede llegar a tener las fallas de seguridad sobre dicho institución, para lo cual la responsabilidad de alta gerencia es fundamental.

Además, los delitos cibernéticos tiene con objetivo dañar activos informáticos, ordenadores, servidores, redes de internet para el caso la Clínica Santa Martha de La Libertad, la información de los pacientes, médicos, antes se manejaban de manera manual

en papeles y en la actualidad en archivos digitales en bases de datos sobre historias clínicas de pacientes, citas, consultas y archivos con información de departamentos como administrativa, recepción, consulta general, además que en ocasiones se presentan inconvenientes en asignar la misma dirección IP en las maquinas generando que no se produzca conexión en la red, por esto se requiere efectuar un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27002 que debilite la probabilidad de ocurrencia de delitos informáticos del área administrativa y de citas médicas de la clínica.

1.2 DESCRIPCIÓN DEL PROYECTO

Cuando los sistemas carecen de un seguimiento de gestión de seguridad en la información, se corre el riesgo de que la información como historias clínicas de los pacientes sean manipuladas o lo que es peor puedan ser robadas, alterar los datos del registro electrónico de los pacientes, cambiar resultados de pruebas, por lo tanto, es fundamental que exista un análisis al sistema el cual proponga un control sobre la manipulación de los datos.

El siguiente estudio se llevará a cabo de acuerdo con la normatividad ya antes descrita, adicionalmente se desarrollará un análisis de las amenazas, donde se clasificarán los procesos más críticos del área de TI. La clínica debe formalizar controles que se dejarán planteados al finalizar el proyecto y de esta manera puedan ejecutar un plan de continuidad que se mantiene en todos los aspectos con procedimientos que ayudan a reducir, mitigar, aceptar o transferir los riesgos identificados.

La seguridad informática se centra en la protección de los activos informáticos de toda clínica, siendo la red de la información interna una parte principal para la protección del recurso más importante “los datos”.

El presente trabajo investigativo busca elaborar un plan de seguridad informático alineado con la normativa ISO 27002 en la institución, para conocer el estado organizacional respecto a la seguridad informática, nos apoyamos en la herramienta informática Kali Linux con herramientas de análisis de vulnerabilidades NMAP, NIKTO, OWASP y aplicamos el estándar ISO para el control de posibles riesgos. Se basa en llevar una auditoria donde a partir del análisis, escaneo de información se conocerá amenazas, los riegos por categorías sean estos altos, medios y bajos. Se establece fases importantes

para el control de la seguridad dentro de la clínica, especificando los roles por fases que nos llevaran a conocer los activos, procesos, todo el funcionamiento de la clínica para la reducción de incidentes de seguridad.

Fase 1: Organización y su contexto

La clínica cuenta con equipo médico de las distintas ramas de la medicina, para brindar un servicio de calidad y calidez humana en una infraestructura acogedora. Dando atención a la comunidad Peninsular desde el 17 de enero del 2009, con una trayectoria que nos ha hecho ganar la estima de nuestros usuarios.

La clínica actualmente cuenta aplicaciones web, servidores marca DELL, Switch, Router, Computadores, Teléfonos Ip, para el manejo de la información tanto de pacientes, usuarios, activos, todo de manera interna, la topología de red es estrella divida en departamentos. TI, Recepción, Medicina General, Administración.

FASE 2 Evaluación de seguridad de la información

A través de la recopilación de información se identifican los activos tecnológicos de información con los que cuenta la clínica, en las aplicaciones de los procesos a evaluar en los posibles riesgos. En la evaluación de los activos de información, se identificarán las amenazas de alto riesgo. Se aplica la norma ISO 27002 de seguridad, sobre los controles a efectuar antes esos posibles riesgos y mitigarlos.

FASE 3 Reportes

La fase de reportes de acuerdos a las amenazas analizadas en los servidores web de la clínica, el reporte describe la amenaza, y posible solución para controlarlo, y para la aplicación de los controles.

FASE 4 Monitoreo y Revisión

En esta fase se basa en la presentación de los resultados, de acuerdo a los procesos de gestión de amenazas en el monitoreo de los controles propuestos antes estos riesgos.

1.3 OBJETIVOS DEL PROYECTO

1.3.1 OBJETIVO GENERAL

- Analizar los posibles riesgos, amenazas del sistema informático de citas, consultas e historiales, mediante la norma ISO 27002 para mejorar la confiabilidad en las áreas de la clínica.

1.3.2 OBJETIVOS ESPECÍFICOS

- Analizar las vulnerabilidades de los datos utilizando el sistema operativo Kali Linux, con las herramientas que dispone como NMAP, NIKTO, OSWAP permitiendo que las amenazas sean identificadas.
- Diagnosticar las posibles amenazas y vulnerabilidades en el servidor web donde se encuentra el proceso de citas clínica de la institución.
- Definir potenciales amenazas que puedan causar perdidas de información en la institución.
- Seleccionar controles de la norma ISO/IEC 27002 que conlleve a la mitigación de las vulnerabilidades encontradas.

1.4 JUSTIFICACIÓN DEL PROYECTO

Después de haber observado los problemas que enfrenta la Institución, es necesario aprovechar al máximo los recursos tecnológicos disponibles para administración y manejo de los datos, sin embargo, la tecnología trae consigo una serie de amenazas que pueden comprometer la información que maneja, como, por ejemplo: los virus, el espionaje, intrusiones y demás delitos informáticos: por tal motivo, es fundamental hacer uso de normas y políticas de seguridad que ayuden a mitigar las amenazas a los que está expuesta los sistemas de la institución.

Por lo tanto, utilizamos la Norma ISO 27002, con la cual se diseñará la política de seguridad, que permite cumplir los objetivos propuestos en la institución. La importancia de realizar un análisis de la seguridad, ayudará al desarrollo del plan de seguridad informática y será de gran ayuda para los encargados de telemática en el aseguramiento de la información que circula por la red.

El desarrollo de este proyecto beneficiará y fortalecerá la seguridad de la red, sitios web de la institución, y por ende se beneficiarán los usuarios que soliciten los diferentes servicios disponibles en la red.

Se proponen algunas de las políticas de seguridad, según la norma ISO 27002

- Políticas de la seguridad de la información

  Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes [3]

- Seguridad de los recursos humanos

Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran [3].

- Gestión de activos

Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas [3]

- Control de acceso

Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información [3]

- Seguridad física y del entorno

Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización [3]

- Seguridad de las operaciones

Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información [3]

- Adquisición, desarrollo y mantenimiento de sistemas

Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes publicas [3]

1.5 ALCANCE DEL PROYECTO

El proyecto de análisis de amenazas y vulnerabilidades basado en norma ISO 27002 para el sistema en el proceso de citas clínicas en la Ciudad de la Libertad, tiene como alcance escanear y solucionar las vulnerabilidades, riesgos del sistema informático de la clínica a la que está expuesta la información, por falta de aplicación de controles de seguridad. La ejecución del análisis de amenazas dará a conocer el nivel de impacto que tendría la materialización de las amenazas identificadas e identificación de criticidad del proceso de citas médicas de la clínica para los activos de información del que pueden afectar datos relevantes a las actividades propias del negocio. La elaboración de matriz de los activos de información que soportan el proceso critico de Citas médicas y posteriormente la identificación de los riesgos de nivel alto, medio y bajo. Y por último la definición de controles según la normativa para mitigar los riesgos identificados a base del análisis de los procesos.

Para realizar el diseño un SGSI que correspondan a las necesidades de seguridad de información para la protección de los archivos que por algunas circunstancias que al ser alterados pueden generar perdidas de las historias clínicas, citas de pacientes, errores en las citas.

Con los resultados de los riesgos existentes y de los activos que se involucran antes las pérdidas de información, por medio del proyecto se espera minimizar, controlar las amenazas empleando controles de seguridad de la norma ISO 27002 lo cual ayuda a fortalecer tres aspectos importantes: la confidencialidad, integridad y disponibilidad de la información que corresponda a las necesidades de seguridad informática, de esta forma tendremos una protección de los datos de la Clínica- Ciudad La Libertad, una vez aplicada políticas de seguridad informática mejorando los niveles de seguridad de la información de los procesos de la clínica.

Contará con información detallada en los siguientes ítems:

- Lista de activos de información relacionados con el proceso a evaluar.
- Información de las amenazas que afectan cada activo involucrado en el proceso.

Limitaciones

Se encuentran relacionadas con las actividades planeadas en cronograma de trabajo previamente definido:

- El escaneo de puertos, vulnerabilidades se realiza de manera interna (clínica)
- El análisis de riesgos se enfocará únicamente en citas, historial clínica.
- No se realizará implementación de ningún control

CAPÍTULO 2

1. MARCO TEORÍCO Y METODOLOGÍA DEL PROYECTO

1.1 MARCO TEÓRICO

Seguridad Informática

Se refiere a los procedimientos implementados para fortalecer la seguridad de los recursos tanto físicos como lógicos de un sistema informático con el fin de evitar que se vea comprometido el principio de autentificación garantizando que quienes acceden a la información son realmente los autorizados para ello. Entre estos se encuentran los servidores, equipos de cómputo, software, bases de datos y los entornos físicos donde se encuentran ubicados dichos elementos [4].

La seguridad informática tiene como objetivo garantizar los mencionados pilares para la seguridad de la información mediante la aplicación de un conjunto de controles que pueden ser físicos como los controles de acceso, cuartos de servidores. También se pueden generar controles a nivel lógico con la utilización de software y controles de acceso como claves de usuarios, biometría, etc. Si bien es claro que la información se puede presentar en una gran variedad de formatos, destacan los físicos y en especial en la actualidad, el formato digital [4].

Vulnerabilidades Informáticas

Son los fallos de los sistemas de seguridad o en los propios que el usuario utiliza para desarrollar las actividades que permitirían que una amenaza tuviese éxito a la hora de generar un problema. El principal trabajo de un responsable de la seguridad es la evaluación de los riesgos identificado las vulnerabilidades, amenazas en base a esta información evaluar los riesgos a los que están sujetos las actividades y recursos [5].

Amenazas

Una amenaza se refiere a un incidente nuevo o recién descubierto que tiene el potencial de dañar un sistema o su empresa en general. Una amenaza es un evento hipotético en el

que un atacante usa la vulnerabilidad. La amenaza no es un problema de seguridad que existe en una implementación u organización. En cambio, es algo que puede violar la seguridad. Esto se puede comparar con una vulnerabilidad que es una debilidad real que se puede explotar [6].

Tipos de amenazas

Las amenazas pueden clasificarse en dos tipos:

Intencionales, en caso de que deliberadamente se intente producir un daño (por ejemplo, el robo de información aplicando la técnica de trashing, la propagación de código malicioso y las técnicas de ingeniería social) [7].

No intencionales, en donde se producen acciones u omisiones de acciones que, si bien no buscan explotar una vulnerabilidad, ponen en riesgo los activos de información y pueden producir un daño (por ejemplo, las amenazas relacionadas con fenómenos naturales) [7].

Amenazas Humanas: La mayoría de estas acciones pueden causar grandes pérdidas.

Ataques activos: obtención de información sin alterarla, difíciles de detectar, ya que no dejan mucho rastro. Las más conocidas son los usuarios con conocimientos básicos (Acceden a estos utilizando técnicas muy sencillas) y los Hackers (informáticos expertos que emplean sus conocimientos para comprobar las vulnerabilidades y corregirlas)

Ataques pasivos: manipulación de la información para obtener beneficio, como, por ejemplo: Antiguos empleados de una organización o Crackers y otros atacantes [8]

Análisis de Riesgos Informáticos

el análisis de riesgos informáticos es la evaluación de los distintos peligros que afectan a nivel informático y que pueden producir situaciones de amenaza al negocio, como robos o intrusiones que comprometan los datos o ataques externos que impidan el funcionamiento de los sistemas propiciando periodos de inactividad empresarial. El análisis y gestión de los riesgos previene a las empresas de este tipo de situaciones negativas para su actividad y recoge una serie de factores fundamentales para su consecución [9].

Identificación de activos

Para realizar un análisis de riesgos efectivo, el primer paso es identificar todos los activos

de la empresa. Estos activos incluyen todos los recursos relacionados con la gestión e intercambio de información de la empresa, como software, hardware, vías de comunicación, documentación digital y manual e incluso de recursos humanos [9].

Principales Características Kali Linux

Kali Linux es una distribución la cual contiene su propia colección de cientos de herramientas de software, especialmente hechas a medida para los usuarios; como profesionales en pruebas de penetración y otros profesionales de seguridad. También viene con un programa de instalación para completamente configurar Kali Linux como el sistema operativo principal en cualquier computadora [10].

Es muy parecido a todas las otras distribuciones Linux existentes, pero existen otras características las cuales diferencian a Kali Linux, muchas de las cuales se adaptan a necesidades específicas de los profesionales en pruebas de penetración [10].

NMAP

Es un software que contiene código abierto y nos sirve para rastrear puertos abiertos, para realizar exploración de redes, sistemas operativos y buscar vulnerabilidades de los mismos, ya sea para realizar informes o realizar ataques [11]

En la imagen podemos observar algunos de los puertos abiertos de la aplicación de la clínica usando en comando NMAP seguido de la dirección IP 209.133.200.122 ó también usando el comando NMAP -T4 -F 209.133.200.122

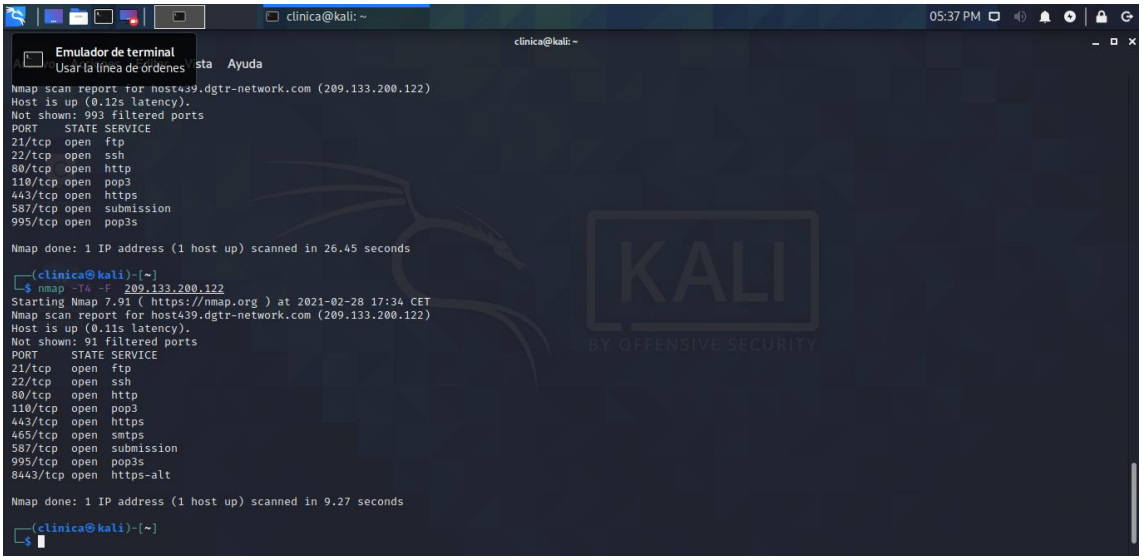


imagen 1 Resultado de análisis con NMAP

Sudo NMAP -0 209.133.200.122

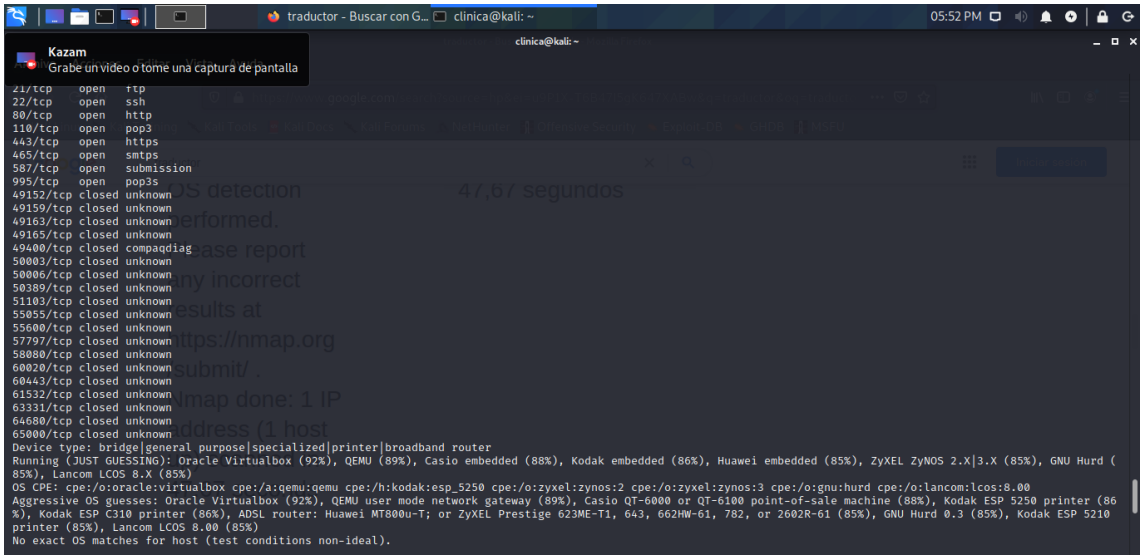


imagen 2 Detalle de los sistemas operativos utilizados

NIKTO

Es una herramienta de escaneo de servidores web que se encarga de efectuar diferentes tipos de actividades tales como, detección de malas configuraciones y vulnerabilidades en el servidor objetivo, detección de ficheros en instalaciones por defecto, listado de la estructura del servidor, versiones y fechas de actualizaciones de servidores, tests de vulnerabilidades XSS, ataques de fuerza bruta por diccionario, reportes en formatos txt, csv, html [12] . Atreves del comando Nikto -h podemos observar vulnerabilidades + OSVDB-3268: / icons /: indexación de directorio encontrada.

+ OSVDB-3233: / icons / README: Se encontró el archivo predeterminado de Apache.

+ OSVDB-3233: /info.php: PHP está instalado y se encontró un script de prueba que ejecuta phpinfo (). Esto proporciona mucha información del sistema.

+ OSVDB-3268: / icons /: indexación de directorio encontrada.

+ OSVDB-3233: / icons / README: Se encontró el archivo predeterminado de Apache.

+ OSVDB-5292: /info.php?file=http://cirt.net/rfiinc.txt

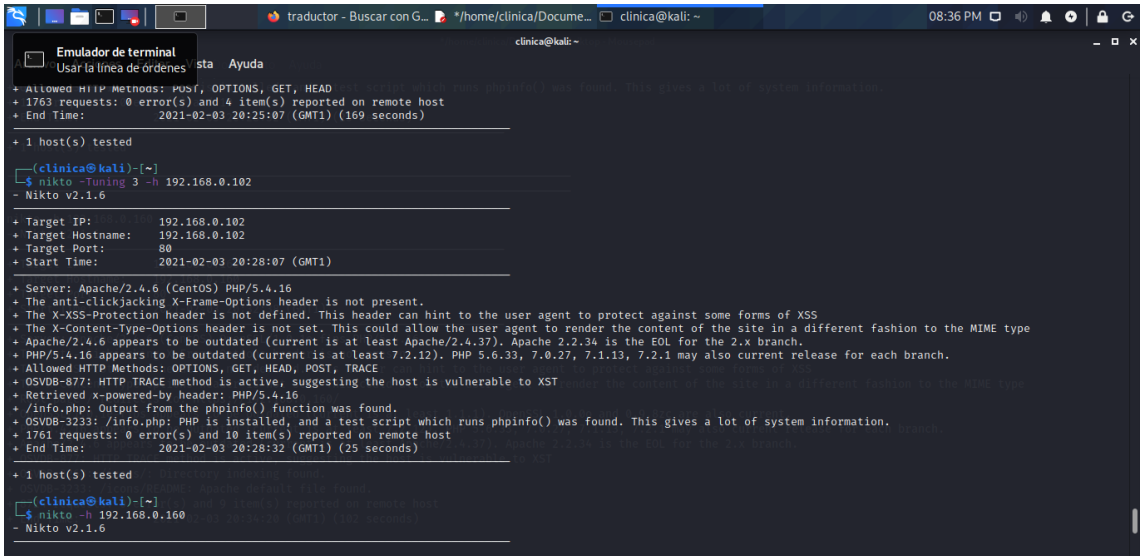


imagen 3 resultados de vulnerabilidades

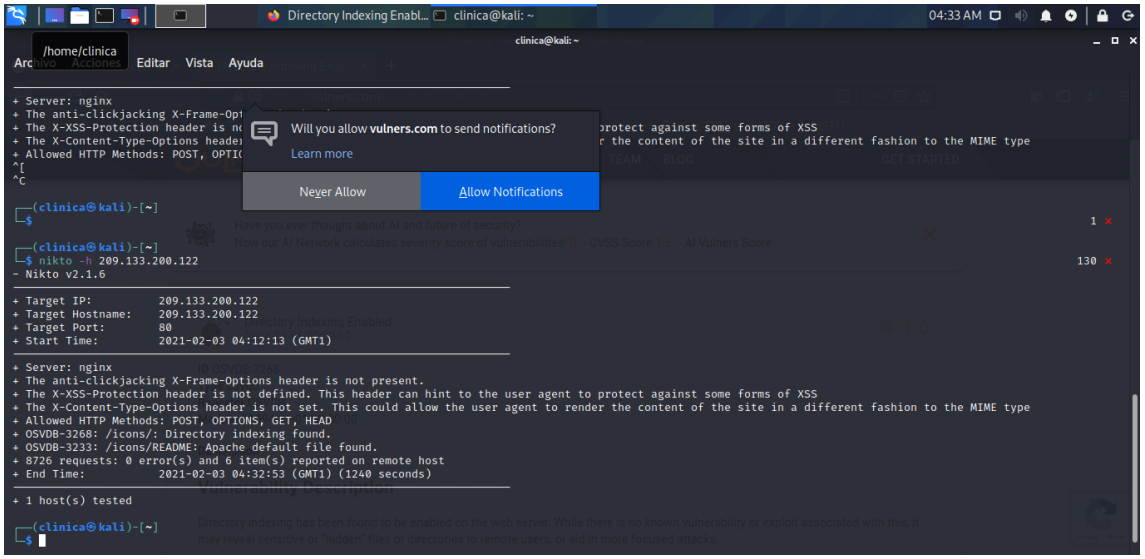


imagen 4 Uso de Herramientas NIKTO para vulnerabilidades

MATELGO

Es una herramienta para recopilar información en la web, y la potencia que posee, permite hallar perfiles en cualquier red social que levanten alguna sospecha de operaciones malintencionadas. Es capaz de hacer búsquedas de dominios, direcciones de correo electrónico, números telefónicos, etc. [13]

HARVESTER

Es una herramienta para conseguir información sobre emails, subdominios, hosts, nombres de empleados, puertos abiertos, banners, desde fuentes públicas como son los motores de búsqueda, servidores PGP, la red social LinkedIn y la base de datos de

SHODAN (Buscador parecido a Google, pero con la diferencia que no indexa contenido, si no que registra cualquier dispositivo conectado a Internet) [14].

Seguridad de la Información

Por seguridad de la información se entiende el conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información. Dicho de otro modo, son todas aquellas políticas de uso y medidas que afectan al tratamiento de los datos que se utilizan en una organización. La seguridad de la información es una pieza fundamental para que la empresa pueda llevar a cabo sus operaciones sin asumir demasiados riesgos, puesto que los datos que se manejan son esenciales para el devenir del negocio. Además, también hay que tener en cuenta que la seguridad de la información debe hacer frente a los riesgos, analizarlos, prevenirlos y encontrar soluciones rápidas para eliminarlos si se diera el caso [15].

¿En que se basa la seguridad de la Información?

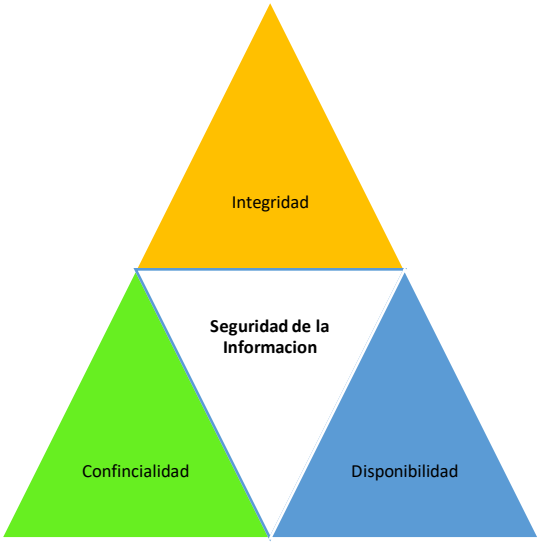


imagen 5. Seguridad de la Información

Disponibilidad

Acceso a la información cuando se requiere, teniendo en cuenta la privacidad. Evitar "caídas" del sistema que permitan accesos ilegítimos, que impidan el acceso al correo [15].

Confidencialidad
Información accesible solo para personal autorizado. La información no debe llegar a personas o entidades que no estén autorizados [15].

Integridad
Información correcta sin modificaciones no autorizadas ni errores. Se protege frente a vulnerabilidades externas o posibles errores Humanos [15]

Norma ISO 27002

La norma ISO 27002 proporciona diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables para iniciar, implementar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como "la preservación de la confidencialidad, integridad y disponibilidad. Establece un conjunto de actividades y directrices bien definidos para la implementación de la seguridad informática, a fin de proteger los activos de informáticos, generando confianza tanto al cliente interno como al cliente externo, de esta manera se empieza a implementar los procesos de seguimientos en cada una de las áreas, estableciendo e identificando cada uno de los potenciales riesgos que se pueden presentar en la empresa. La norma ISO 27002 se encuentra organizado en base a los 14 dominios, 35 objetivos de control y 114 controles [16]

El objetivo que persigue la norma ISO 27002 es que la organización conozca de forma precisa todos los activos que posee. Esta información es una parte muy importante de la administración de riesgos.
Algunos ejemplos de activos son:
Recursos de información: bases de datos y archivos, la documentación de los sistemas, los manuales de usuario, el material utilizado durante la capacitación, los procedimientos operativos, los planes de continuidad y contingencia, etc.
Recursos de software: software de aplicaciones, sistemas operativos, herramienta utilizadas para llevar a cabo los desarrollos, etc.
Activos físicos: equipamiento informático, equipos de comunicación, mobiliario, etc.
Servicios: los servicios informáticos y de comunicaciones [16].

2.2 METODOLOGÍA DEL PROYECTO

Se utilizó la metodología diagnostica y exploratoria, para la recopilación de información de los procesos y servicios que maneja la Clínica “Santa Martha”.

Se realizo un estudio investigativo de tipo exploratorio ya que se llevará a cabo las diferentes técnicas de recopilación de información, consultar los problemas a los que se enfrenta la institución ya que anteriormente no se ha realizado un análisis de amenazas y vulnerabilidades informática en la institución.

El estudio investigativo es de tipo exploratorio ya que se llevará a cabo las técnicas para la recopilación de información, también buscar información similar de fuentes para establecer la estructura del problema, esto genera ayuda para realizar el análisis de los procesos en los sistemas y las referencias que ayuda que ha utilizado el investigador.

Para este caso de Análisis de amenazas y vulnerabilidades informáticas basado en la Norma ISO 27002, para una Institución, se utilizó las herramientas de entrevista, reuniones para recolección de información, para la medición de vulnerabilidades, amenazas, riesgos en cuantos a la confidencialidad, integridad y disponibilidad de la información.

Además, se realiza una investigación diagnóstica este tipo de investigación identifica los factores que intervienen en la institución, los problemas, funciones, procesos para generar una idea global del contexto del objeto de estudio y consecuencias, así permitir que las decisiones en función de los datos recopilados y analizados.

2.3 METODOLOGÍA DE EVALUACIÓN DE SEGURIDAD DEL SISTEMA DE INFORMACIÓN (ISSAF)

Para el proyecto se establece la metodología ISSAF de OISSG (Open Information System Security Group), puesto que está basada en la evaluación y análisis de seguridad de redes y aplicativos [17]. Los lineamientos de la metodología se enfocan en tres fases siguientes:

Planificación y Preparación: En esta fase comprende los pasos iniciales para el intercambio de información, planificar y prepararse para la prueba. Antes de llevar a cabo la prueba formal de acuerdo será firmado por las ambas partes. Que constituye la base de esta tarea y la mutua protección jurídica [17].

Evaluación: Esta es la fase en donde lleva acabo el test de penetración. En la fase se realiza la recolección de Información, Identificación de vulnerabilidades, Obtener Acceso y escalada de privilegios [17]**.**

Reportes: Se emitirán reportes del análisis que se realizó en los sistemas para detallar cada uno de los softwares maliciosos encontrados en el servidor web [17].

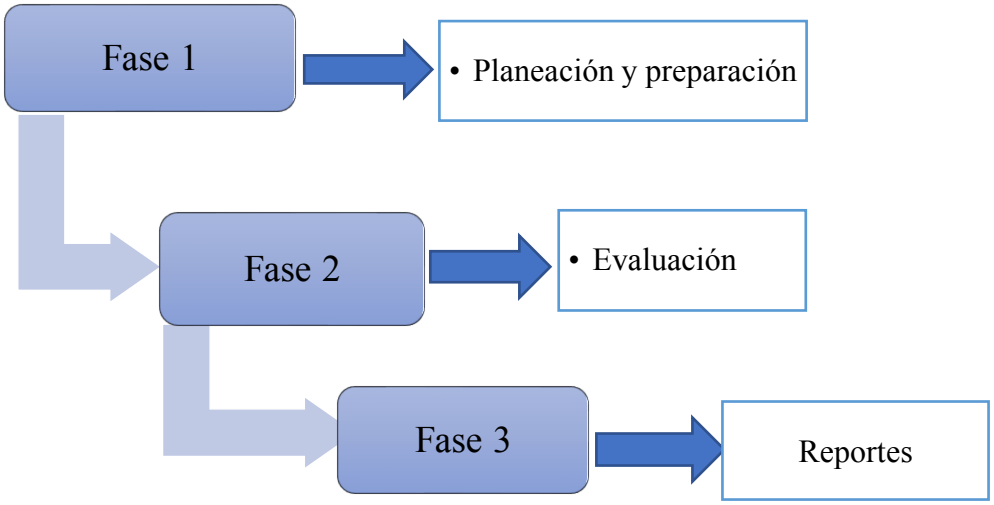


imagen 6 Metodología ISSAF

2.4 TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Para la realización de proyecto de análisis de amenazas y vulnerabilidades basado en Norma ISO 27002, se toma en cuentas las siguientes técnicas de investigación y métodos:

Las técnicas e instrumentos de investigación son las actividades a realizar que nos llevará a cumplir con los objetivos que planteamos para la realización de nuestro proyecto de investigación. Las técnicas de investigación para la recopilación de información que nos llevará a realizar el análisis de vulnerabilidades serán las siguientes:

Observación: con esta técnica de investigación se realizó un estudio de los procesos más frecuentes que se realizan la institución, también se realizará las encuestas para la recopilación de información.

Entrevistas: Para la recolección de información también fue fundamental el uso de entrevistas a una o más trabajadores de la clínica, y los beneficios que lograrían la institución al realizar el análisis en los sistemas.

Se espera que al aplicar estos instrumentos se determinen las causas reales de amenazas y vulnerabilidades a las que se expone la información de la institución, y de esta forma aplicar la norma ISO 27002. A través de las técnicas de recolección de información en la institución se accedió a la información y activos de información que manejan para el análisis informático en los procesos específicamente en el proceso de consultas.

CAPÍTULO 3

PROPUESTA

Para el desarrollo del análisis en la institución es necesario realizar 4 fases fundamentales que nos lleva al seguimiento de amenazas, vulnerabilidades informáticas basada en la norma ISO 27002 en La Clínica Santa Martha, Ciudad La Libertad, los pasos para la metodología son los siguientes:

3.1 FASE 1: ORGANIZACIÓN, PLANIFICACIÓN Y PREPARACIÓN

Santa Martha es una clínica de tipo privado, que brinda servicios de consultas pediatras, ginecólogo, atenciones hospitalarias, cirugías en general, cirugías laparoscopia, artroscopias, Laboratorio clínico, ecografías – resonancia y RX

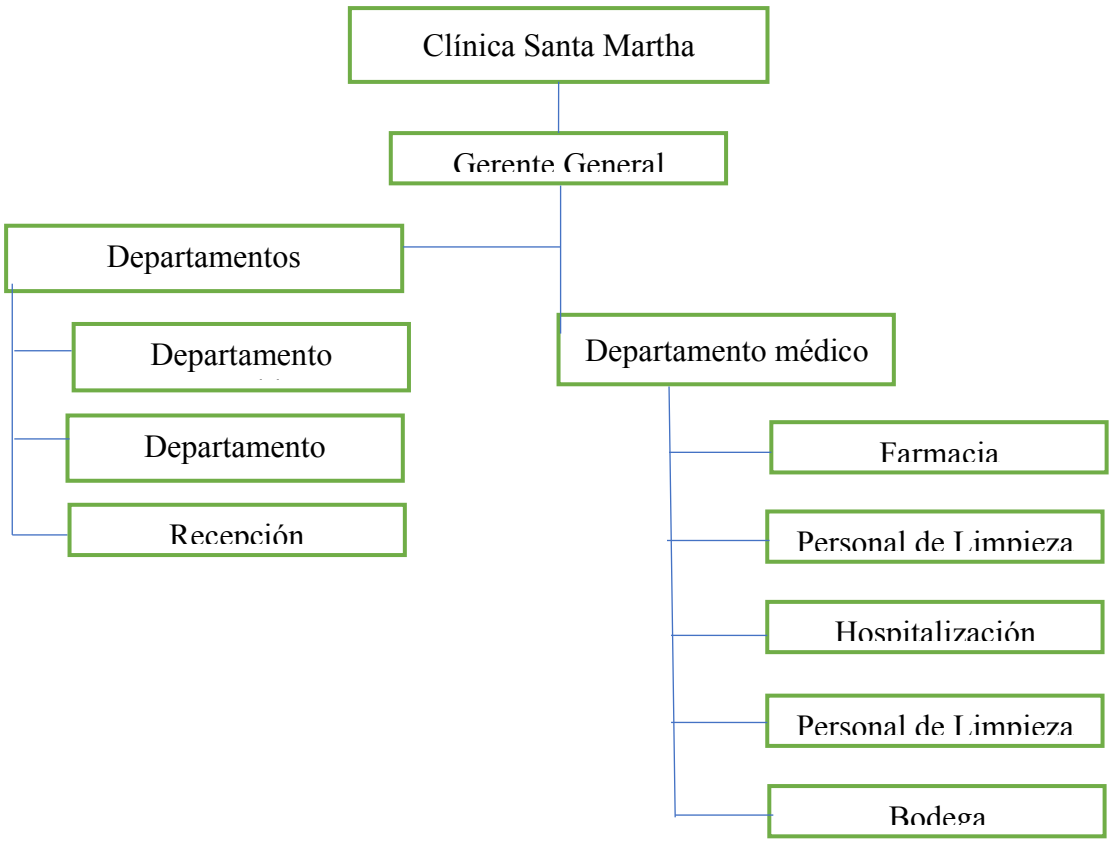


imagen 7 Organización de la empresa

3.2 FASE2: EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN

La clínica cuenta con diferentes procesos, el análisis informático se realiza en el proceso de citas y consultas médicas.

PROCESOS DE LA CLINICA

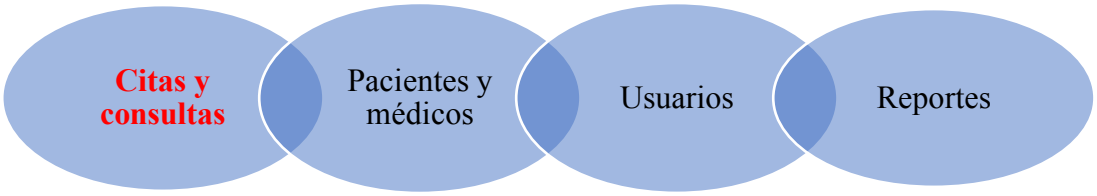


imagen 8 Procesos

SUBPROCESOS DE LA CLINICA

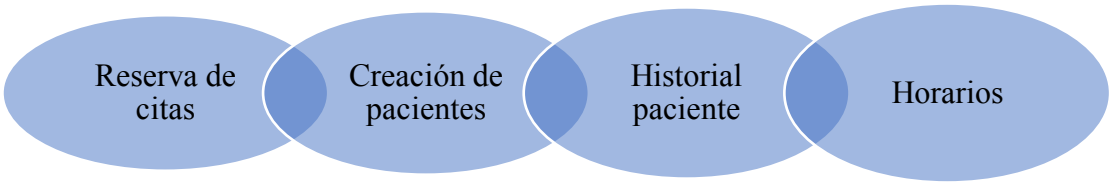


imagen 9 Subprocesos

3.2.1 DIAGRAMA DE FLUJO DE DATOS

PROCESO DE CITAS

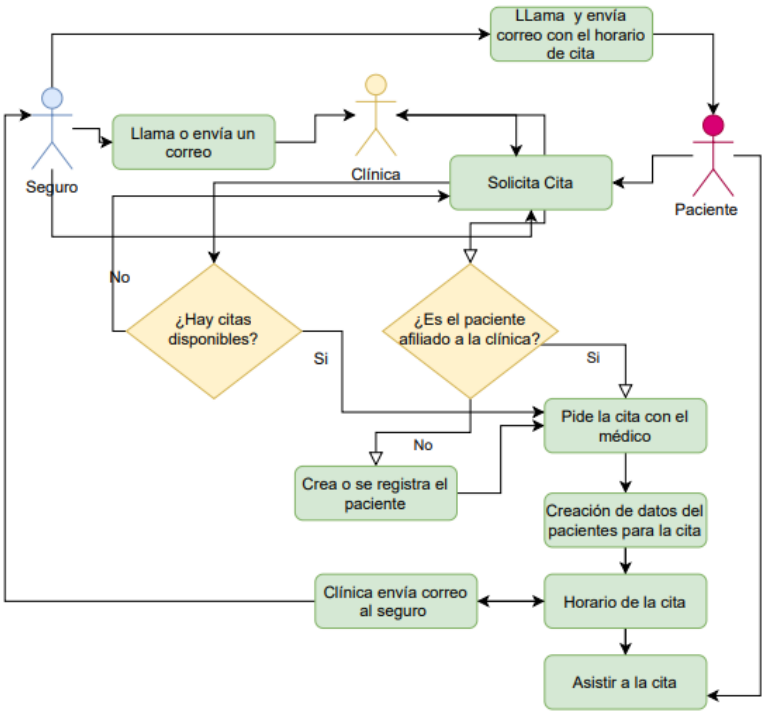


imagen 10 Procesos de Citas

PROCESO DE CITAS

Paciente

- El paciente asiste a la clínica para solicitar una cita.
- ¿El paciente es afiliado? **Si** entonces esta registrado en el sistema.
- ¿El paciente es afiliado? **No** entonces se crea el paciente.
- Se pide la cita.
- Se define la creación y horario de la cita para el paciente
- Asiste a la cita.

Seguro

- El seguro llama o envía correo a la clínica para solicitar una cita.
- ¿El paciente es afiliado? **Si Hay citas disponibles**, se pide la cita con el médico.
- ¿El paciente es afiliado? **No** el seguro vuelve a solicitar citas.
- Se define la creación y horario de la cita para el paciente
- Clínica envía correo de la cita al seguro
- El seguro llama o envía correo de cita al Paciente
- El paciente asiste a la cita.

3.2.2 ESTRUCTURA DE LA RED CLÍNICA

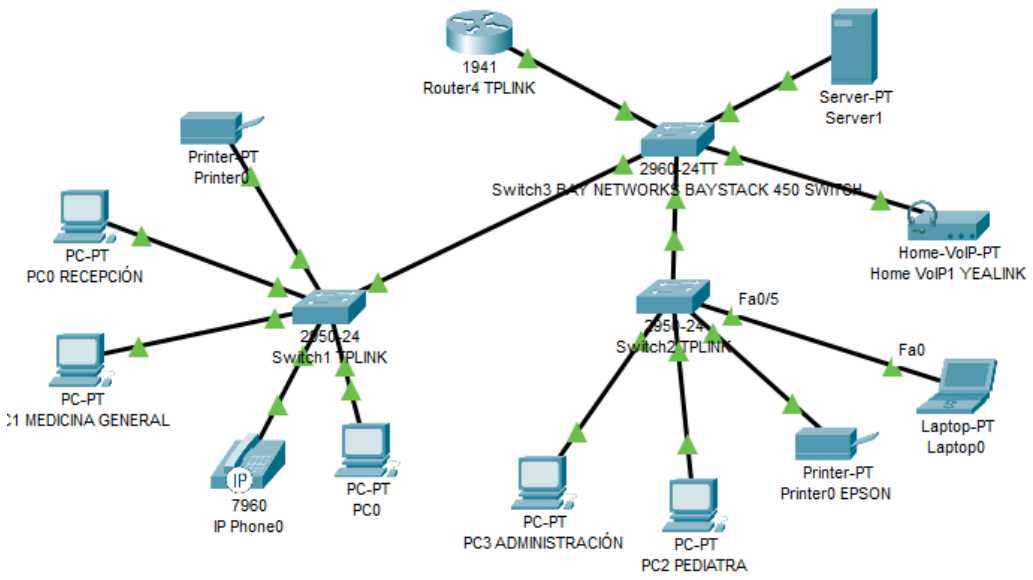


imagen 11 Infraestura de la red

3.2.3 IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

Id	Activos de Información		Descripción
Sis-ser003	SERVIDOR DELL POWEREDGE T140 SERVICE TAG: 7D4JBZ2		Servidor principal que contiene los servidores secundarios y demás equipos
Sis-ser004	SERVIDOR DELL POWEREDGE T140 SERVICE TAG: 7D4JBZ2	SERVIDOR WEB MYSQL APACHE	Aplicativos WEB de la clínica. Carpeta medica Clisamarsa
		SERVIDOR DE BD SQLSERVER	Servidor que contiene los datos módulos de citas, consultas, historial médico, pacientes, etc.
Sis-ser007	SERVIDOR DE IMPRESIÓN HAMLET HPS01UU PRINT SERVER		Impresiones de forma remota en los diferentes departamentos en la clínica
Rec-067	RELOJ BIOMÉTRICOS DE ACCESO – ZTECO		Control de asistencia del personal
Rec-066	SWITCH TP-LINK TL-SG3428		SWITH principal para la Conexión con los dispositivos de la clínica PC, portátil, ROUTER, otro SWITCH, etc.
Rec-067	SWITCH GIGABIT TP-LINK TL-SG1048		Conexión de equipos a la red de la clínica
Rec-035	ROUTER HUAWEI PROVEEDOR NETLIFE		Servicio de Internet 100MB
Rec-023	TELEFONO COMUTADOR PANASONIC KX-T7730		Monitoreo de llamadas internas automáticas
Rec-001	ROUTER TP-LINK		Dispositivo de red para conexión a internet
Sis-ser009	SERVIDOR DE IMPRESIÓN DP-G310		Impresiones de forma remota en los diferentes departamentos en

		la clínica
Sis-act001	CAMARA DE VIGILANCIA TRENDNET TV-IP100 WEBCAM	Control del trabajo y actividad de los empleados
Rec-069	BAY NETWORKS BAYSTACK 450 SWITCH	Conexión de equipos a la red de la clínica

Para realizar la identificación de los activos de información se contó con la ayuda del Ingeniero encargado en el departamento de TI y las cuales nos brindaron la información necesaria.

Tabla 1Identificación de los activos de información

Servidores

Servidor	Memoria RAM	Disco Duro	Marca
Principal	4,8	2 TB	SERVIDOR DELL POWEREDGE T140 SERVICE TAG: 7D4JBZ2
Servidor de BD	4,8	2 TB	SERVIDOR DELL POWEREDGE T140 SERVICE TAG: 7D4JBZ2

Tabla 2 Servidores de la Clínica

SWITCH

SWITCH	Interface	Capacidad de conmutación	Buffer Memory	Velocidad de Reenvío del Paquete	Medios de Red
SWITCH GIGABIT TP-LINK TL-SG1048	48 puertos RJ45 de 10/100/1000Mbps	96Gbps	16Mb	71.4Mpps	10BASE-T: cable UTP categoría 3, 4, 5 (máximo 100m)
SWITCH TP-LINK TL-SG3428	24 puertos 10/100 Mbps	12,8 Gbit/s		9.5Mpps	100BASETX/1000Base-T: cable UTP categoría 5,

					5e, 6 o mayor (máximo 100m)

Tabla 3 SWITCH de la clínica

3.2.4 REPORTES DE LAS VULNERABILIDADES. Ver Anexo

Equipos	Amenaza	Agente de la Amenaza
Servidor Web	Código malicioso	Hacker
	Modificación no autorizada de información	Personal interno inexperto (accidental) Personal interno descontento (intencional) Ex–empleado
	Virus en las redes o computadoras	Hacker
Servidor de Base de Datos	Código malicioso	Hacker
	Modificación no autorizada de información	Personal interno inexperto (accidental) Personal interno descontento (intencional) Ex–empleado
	Virus en las redes o computadoras	Hacker
Router	Virus en las redes o computadoras	Hacker
	Modificación no autorizada de información	Personal interno descontento (intencional)
Switch	Modificación no autorizada de información	Personal interno inexperto (accidental) Personal interno descontento (intencional) Ex–empleado
Servidor de impresión	UPS defectuoso o sin	Personal interno

Servidor línea Telefónica	mantenimiento	descontento (intencional)
	Fallas de hardware en los equipos	Material (falla)

Tabla 4 Listado de amenazas, vulnerabilidades dentro de la clínica

3.3.4 DESCRIPCIÓN DEL TRATAMIENTO DEL RIESGO: 4 estrategias (ACEPTAR, TRANSFERIR, MITIGAR Y EVITAR). Ver ANEXO

ESTRATEGIA	CONTROL PROPUESTO
Mitigar	Antivirus que incluyan actualización automática para la detención, prevención y controles de recuperación para proteger contra código malicioso, configurar contraseñas de alta seguridad, Instalar las últimas versiones de los parches disponibles para el software, servicios de los equipos operativos, cambiar contraseñas de administrador.
Mitigar / Transferir	Controles de acceso biométrico para asegurar que solo se permite el acceso a personal autorizado, cámaras de seguridad al interior y exterior de la clínica en las 3 plantas y departamentos, botón de alarma.
Mitigar	Permiso para el acceso a los archivos, información y las funciones del sistema de aplicación solo para personal autorizado, Capacitación del personal, respaldos de los archivos y datos de la clínica.
Mitigar	Restricción de acceso, capacitación al personal sobre funcionamiento de los equipos, gestión de contraseñas.
Mitigar	Restricción de acceso, capacitación al personal sobre funcionamiento de los equipos, gestión de contraseñas, contratos con el proveedor del servicio.
Mitigar	Eliminación de accesos a la información cuando el empleado finaliza su contrato, respaldo de los datos.
Mitigar	Cambio de contraseñas de nuestros sistemas, actualizar el firmware del Router o todo equipo conectado al ordenador

Transferir	Certificación y actualización de los conocimientos del personal TI, Respaldos externos de la información periódicamente, mantener activado el firewall del equipo, actualización automática estén activadas para recibir actualizaciones de seguridad

Tabla 5 Tratamiento de Riesgos

En el cuadro de tratamiento de riesgo para mitigar su impacto según las amenazas se tiene en cuanta las estrategias (aceptar, transferir, mitigar y evitar)

Aceptar: se emplea la estrategia si un riesgo no es suficientemente critico para la clínica la medida de control puede ser aceptado, es decir no hacer nada para evitarlo. Es apropiada para amenazas de baja prioridad

reducir la probabilidad de que ocurra, reducir su impacto,

Mitigar: Se trata de reducir la probabilidad de que ocurra, reducir su impacto sobre un riesgo

Transferir / Mitigar: Si el riesgo representa una amenaza importante para la seguridad de la información se toma la decisión de transferir o mitigar el riesgo terceras personas o entidad.

Evitar: Si el riesgo es demasiado alto para la clínica lo asuma, puede optar o evitar el riesgo, hacer un cambio en el proyecto, de modo que el riesgo desaparezca.

MONITOREO Y REVISIÓN: DESARROLLO DE POLÍTICAS DE SEGURIDAD NORMA ISO 27002.

Las políticas de seguridad de la información que se deben aplicar en la clínica sede la Libertad, provienen de la recopilación de información, análisis de amenazas de la situación actual. Se proponen algunas de las políticas de seguridad, según la norma ISO 27002

- Políticas de la seguridad de la información
- Seguridad de los recursos humanos
- Gestión de activos
- Control de acceso
- Seguridad física y del entorno
- Seguridad de las operaciones

- Adquisición, desarrollo y mantenimiento de sistemas

POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

A.5.1.1 Políticas para la seguridad de la información

Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.

Listado para aplicar políticas de seguridad de la Información

- Verificar que los cargos en los departamentos con respecto a la seguridad de la información existan roles y responsabilidades en la clínica.
- Los usuarios tendrán el acceso a Internet previa autorización siempre y cuando se cumplan los requisitos mínimos de seguridad para acceder a este servicio y se acaten las disposiciones de conectividad de la unidad informática.
- Capacitación a los usuarios en los temas de seguridad.
- Revisión de manuales políticos sobre el personal que laboran en los departamentos que no existan inconsistencia, en cuanto a las responsabilidades que desempeñan el personal en su área de trabajo.
- El encargado del área de TI debe asegurarse del uso adecuado de los activos de información por el personal. Brindar asistencia técnica de hardware y software.

SEGURIDAD DE LOS RECURSOS HUMANOS

A.7.1.2 Términos y condiciones del Empleo

Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.

Listado para aplicar políticas de seguridad de la Información

- La selección de un nuevo empleado para la clínica, existirá un contrato legalizado, el que incluirá cláusulas de confidencialidad, las que debe cumplir ya sea persona natural o jurídica.
- Verificar al personal que controles y responsabilidades presta en los activos de información.

- Los Departamentos deberán estar informados sobre las responsabilidades de seguridad informática, además de sanciones por incumplimiento de las mismas

A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información

Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.

Listado para aplicar políticas de seguridad de la Información

- Se debe realizar capacitaciones, al asignar responsabilidades a cada encargado de departamento en su área. El encargado de organizar este tipo de actividades será el departamento de TI de la clínica para difundir las políticas de seguridad.
- El departamento de sistemas tendrá la responsabilidad de proporcionar capacitaciones que permita la actualización cada cierto tiempo que se vea necesario para estar claro en relación con el tema y cambios que hayan surgido.

GESTION DE ACTIVOS

A.8.3.1 Gestión de medios removibles

Control: Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización

Listado para aplicar políticas de seguridad de la Información

- El uso de medios removibles de almacenamiento solamente es autorizado a los funcionarios de la clínica que son autorizados por Gerencia y TI.
- Los medios de almacenamiento removibles como cintas, discos duros, y dispositivos USB, que contengan información institucional, deben ser controlados y físicamente protegidos por el funcionario responsable de la información.
- La información de la clínica que es almacenada en medios removibles y que debe estar disponible por largo tiempo, es protegida y controlada adecuadamente para evitar que ésta se vea afectada por el tiempo de vida útil del medio.

CONTROL DE ACCESO

A.9.1.1 Política de control de acceso

Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.

Listado para aplicar políticas de seguridad de la Información

- Realizar un cronograma sobre los privilegios concedidos a los usuarios de los departamentos de la clínica.
- Identificar y definir niveles de acceso para empleados de la clínica con labores dentro de su departamento.
- Capacitar y controlar al personal para que tengan buenas prácticas de seguridad en el uso y protección de contraseñas, las cuales permite a los usuarios validar y establecer el derecho de acceso a las instalaciones, equipos y servicios informáticos

A.9.2.1 Registro y cancelación del registro de usuarios

Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso

Listado para aplicar políticas de seguridad de la Información

- Identificar con nombre de usuario que identificará de manera segura para el departamento de la clínica en el que labore, el usuario y el nivel de acceso asignado al empleado le permitirá realizar sus labores dentro de su área de trabajo.
- Solo podrán ingresar a la aplicación web los usuarios que están asignadas a usar el aplicativo.
- Todo usuario que termine su contrato de trabajo, deberá ser notificado para dar de baja en el sistema.

A.9.2.5 Revisión de los derechos de acceso de usuarios

Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.

Listado para aplicar políticas de seguridad de la Información

Con la ejecución de este control se realizarán revisiones de los niveles de acceso que se le concedió a los usuarios de los departamentos de la clínica.

- Control a los usuarios que tengan acceso para verificar que información está autorizada
- Consultar si los empleados realizan respaldo de la información en el departamento en el que labora.

A.9.2.6 Retiro o ajuste de los derechos de acceso

Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.

Listado para aplicar políticas de seguridad de la Información

- Todo usuario que termine su contrato de trabajo, deberá ser notificado para dar de baja todos los permisos y derechos concedidos al usuario en los sistemas.

A.9.4.1 Restricción de acceso a la información

Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.

Listado para aplicar políticas de seguridad de la Información

- En personal que labora en la clínica y tiene acceso al sistema ingresara con su usuario y contraseña.
- Se debe permitir el acceso a la información, que requiera el usuario
- Los usuarios solo tendrán acceso a la información autorizada

SEGURIDAD FÍSICA Y DEL ENTORNO

A.11.1.2 Controles de accesos físicos

Control: Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado.

Listado para aplicar políticas de seguridad de la Información

- Se contará con un registro de cada persona que ingrese a un área determinada con

los datos personales, cedula hora de ingreso y salida.

- Se utiliza acceso biométrico para el personal de la clínica.

A.11.2.4 Mantenimiento de equipos

Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.

Listado para aplicar políticas de seguridad de la Información

- Manteamiento de los equipos de la clínica dando a conocer los posibles daños o cambios realizados.

A.12.2.1 Controles contra códigos maliciosos

Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos

Listado para aplicar políticas de seguridad de la Información

- Los usuarios no deben instalar software no autorizado, ya que este puede ser ilegal o causar inconvenientes en los equipos donde se realice la instalación incluso puede infectar servidor web de la clínica.
- El departamento de TI es el encargado de realizar el monitoreo y actualización de los programas como antivirus y los usuarios deberán reportar a este departamento sobre cualquier problema.

A.12.7 Controles de auditorías de sistemas de información

Control: Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.

Listado para aplicar políticas de seguridad de la Información

- Id de Usuario
- Hora y fecha de ingreso y salida
- Hora y fecha de actualización
- Nombre del equipo donde se realizó la sesión

- Obtener un registro de accesos fallidos y de ingresos.
- Monitoreo de los accesos a utilidades, aplicaciones y departamentos.

Control	Riesgo mitigado	Descripción
A.5.1.1 Políticas para la seguridad de la información	Todos los riesgos	La institución definirá un conjunto de políticas para la seguridad de la información, aprobada por el directorio principal, publicada y comunicada a los colaboradores y a las partes externas pertinentes.
A.7.1.2 Términos y condiciones del Empleo	Modificación no autorizada de información Acceso no autorizado	Control de los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información
A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información	Modificación no autorizada de información Respaldos defectuosos	Los empleados de la clínica, recibirán capacitaciones sobre la conciencia y actualización de las políticas y procedimiento de la organización. Que sean relevantes para la función laboral.
A.8.3.1 Gestión de medios removibles	Código malicioso Virus en las redes o computadoras	Definir y aprobar procedimientos para la gestión y uso de medios extraíbles, tales como: memorias USB, discos duros externos, CD.
A.9.1.1 Política de control de acceso	Código malicioso Modificación no autorizada de información Acceso no	Establecer, almacenar, revisará una política de control de acceso de usuarios basado en los privilegios de seguridad de la institución

	autorizado	
A.9.2.1 Gestión de altas/bajas en el Registro de usuarios	Código malicioso Modificación no autorizada de información	Permitir la asignación de derechos de acceso a usuarios para la administración.
A.9.2.2 Suministro de acceso de usuarios	Código malicioso Modificación no autorizada de información	Proceso formal de provisión de acceso a los usuarios para asignar derechos de accesos para todos los tipos de usuarios a sistemas y servidores.
A.9.2.5 Revisión de los derechos de acceso de usuarios	Código malicioso Modificación no autorizada de información	Definir y aprobar un procedimiento para la revisión periódica de los derechos de acceso de usuarios por parte de los propietarios de los activos de información.
A.9.2.6 Retiro o ajuste de los derechos de acceso	Código malicioso Modificación no autorizada de información	Definir y aprobar un procedimiento para la revocación de derechos de acceso de los usuarios al terminar su empleo o vinculación con la institución.
A.9.3.1 Uso de información de autenticación secreta	Código malicioso Modificación no autorizada de información	Los usuarios deben cumplir políticas de contraseñas en la clínica, que son aplicadas en el sistema
A.9.4.1 Restricción de acceso a la información	Código malicioso Modificación	Se refiere al estándar de contraseña y autentificación.

	no autorizada de información	
A.9.4.2 Procedimiento de ingreso seguro	Código malicioso Modificación no autorizada de información	Se debe solicitar usuario y contraseña al ingresar a los sistemas y aplicaciones.
A.9.4.5 Control de acceso a códigos fuente de programas	Modificación no autorizada de información	El acceso al código fuente de los programas debe ser restringido únicamente a usuarios autorizados.
A.10.1.1 Política sobre el uso de controles criptográficos	Código malicioso	Definir y aprobar una política para el uso de controles criptográficos, tales como: certificados digitales, cifrado de claves, etc.
A.11.1.2 Controles de acceso físico	Modificación no autorizada de información Negación de servicio	Implementación de controles de acceso y protección física, tales como: acceso biométrico, puerta de acero, ascensor, cámaras de seguridad al interior y exterior, alertas
A.11.2.4 Mantenimiento de equipos	UPS defectuoso o sin mantenimiento	Plan de mantenimiento de equipos de cómputo. Contrato con el proveedor para el mantenimiento del UPS.
A.12.1.1 Procedimientos de operación documentados	Modificación no autorizada de información	Documentar los procedimientos del área de Tecnología, incluidos los procedimientos de gestión de la seguridad física y lógica.
A.12.2.1 Controles contra códigos maliciosos	Código malicioso Modificación no autorizada de información Virus en las	Adquisición y configuración de antivirus corporativo para todos los equipos de la red institucional. Revisión y actualización de las reglas del firewall existente.

	redes o computadoras	
A.12.5.1 Instalación de software en sistemas operativos	Código malicioso	Configurar mediante reglas del Directorio Activo existente, restricciones para instalación de software no autorizado.
A.12.7 Controles de auditorías de sistemas de información	Código malicioso Fraude	Ejecución de auditorías de sistemas, al menos una vez al año.
A.14.2.1 Política de desarrollo de software	Código malicioso	Elaborar una política que incluya las directrices para el desarrollo de sistemas en la institución.
A.14.2.5 Principios de construcción de los sistemas seguros	Código malicioso Fallas de Hardware en los equipos	Establecer, documentar, y mantener principios para la construcción de sistemas seguros y aplicarlos a cualquier actividad de implementación de sistemas.
A.14.2.6 Ambiente de desarrollo seguro	Código malicioso	Mantener segregados los ambientes de pruebas y producción con los debidos controles de acceso.
A.18.2.1 Revisión independiente de la seguridad de la información	Código malicioso Modificación no autorizada de información	Contratar un análisis de ethical hacking al menos una vez al año.

Tabla 6 Plan de Acción y Controles ISO/IEC 27002

CONCLUSIONES

- Con la información recolectada en la clínica, se identificó los activos de información que están expuestos amenazas no intencionales, modificación de información no autorizadas que se basan a errores de usuarios por lo que es necesario utilizar normas de seguridad según la normativa ISO 27002.
- A través de las herramientas de análisis de vulnerabilidades se evidencio amenazas a la que está expuesta la clínica en los procesos de citas, historial clínico, por lo que es importante aplicar controles para la protección de la información.
- Mediante el uso de herramientas del software libre Kali Linux, identificamos potenciales amenazas, código malicioso que pueden alterar la información de los procesos de la clínica.
- Para mitigar, controlar, eliminar los riesgos que ocasiones inconvenientes en la clínica, se surgiere aplicar las medidas y controles que se proponen en la documentación de las políticas de seguridad de la Normativa ISO 27002, esto requiere inversión y aprobación de alta gerencia para la ejecución.

RECOMENDACIONES

- Se debe estar en constate actualización en el proceso de gestión de seguridad de la información, debido a las nuevas amenazas que circulan diariamente, que afectan al sistema de información.
- Crear procesos de revisión periódicos de amenazas, vulnerabilidades mediante la metodología ISSAF, efectuado en la documentación para la mitigación a futuro.
- A la Gerencia que se aplique las políticas de seguridad realizada en la documentación de los controles y políticas para llevar una protección en la información de la clínica.
- Contratación periódica de un analista de seguridad de la información, quien se encargará del monitoreo, seguimiento de la seguridad informática mediante el uso de herramientas de software, y velar por el cumplimiento de los controles y políticas establecidos en el plan de seguridad de la información.

BIBLIOGRAFÍA

[1] L. X. S. b. ALEJANDRO JIMÉNEZ, *ANÁLISIS DE RIESGOS, AMENAZAS Y VULNERABILIDADES,* Bogota, 2016.

[2] A. Moscoso, *Elaboración y plan de implementación de políticas de seguridad de la información aplicadas a una empresa industrial,* Cuenca, 2017.

[3] I. 27002:2013, *Information Technology. Security Techniques. Code of Practice for,* Colombia: Instituto Colombiano de Normas Tecnicas y Certification (I, 2013.

[4] J. González Londoño, *Estudio del estado actual de la seguridad informática en las organizaciones de colombia.,* Bogota, 2020.

[5] M. I. Romero, *Introducción a la seguridad informática y el análisis de vulnerabilidades,* 2018.

[6] A. E. Ortiz, «¿Qué es una amenaza informática?,» 13 julio 2020. [En línea]. Available: https://www.hostdime.la/blog/que-es-una-amenaza-informatica-como-contenerla/. [Último acceso: 11 diciembre 2020].

[7] U. N. d. Luján, «Departamento de seguridad Informatica,» [En línea]. Available: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12. [Último acceso: 11 diciembre 2020].

[8] Andrea, «SEGURIDAD INFORMÁTICA,» 13 Noviembre 2016. [En línea]. Available: https://blogseguridadandrea.wordpress.com/2016/11/13/2-1-tipos-de-amenazas/. [Último acceso: 20 Enero 2021].

[9] P. Rodríguez, «Análisis de riesgos informáticos y ciberseguridad,» 7 mayo 2020. [En línea]. Available: https://www.ambit-bst.com/blog/an%C3%A1lisis-de-riesgos-inform%C3%A1ticos-y-ciberseguridad. [Último acceso: 11 diciembre 2020].

[10] A. Caballero, «Principales Características de Kali Linux,» 21 novuembre 2019. [En línea]. Available: http://www.reydes.com/d/?q=Principales_Caracteristicas_de_Kali_Linux. [Último acceso: 11 diciembre 2020].

[11] M. A. Daza Castillejo, *"Capacidades técnicas, legales y de gestión para equipos blueTeam y redTeam.",* 2020.

[12] A. M. Ortiz Castillo, *"Introducción a las pruebas de penetración.",* 2020.

[13] «Internet paso a paso,» [En línea]. Available: https://internetpasoapaso.com/maltego/. [Último acceso: 18 febrero 2021].

[14] P. J. Olmedo, «Obtener información con The Harvester,» 9 marzo 2015. [En línea]. Available: https://hackpuntes.com/obtener-informacion-con-the-harvester/. [Último acceso: 21 febrero 2021].

[15] «Seguridad de la Informacion,» 2017. [En línea]. Available: https://www.tecon.es/la-seguridad-de-la-informacion/. [Último acceso: diciembre 16 2020].

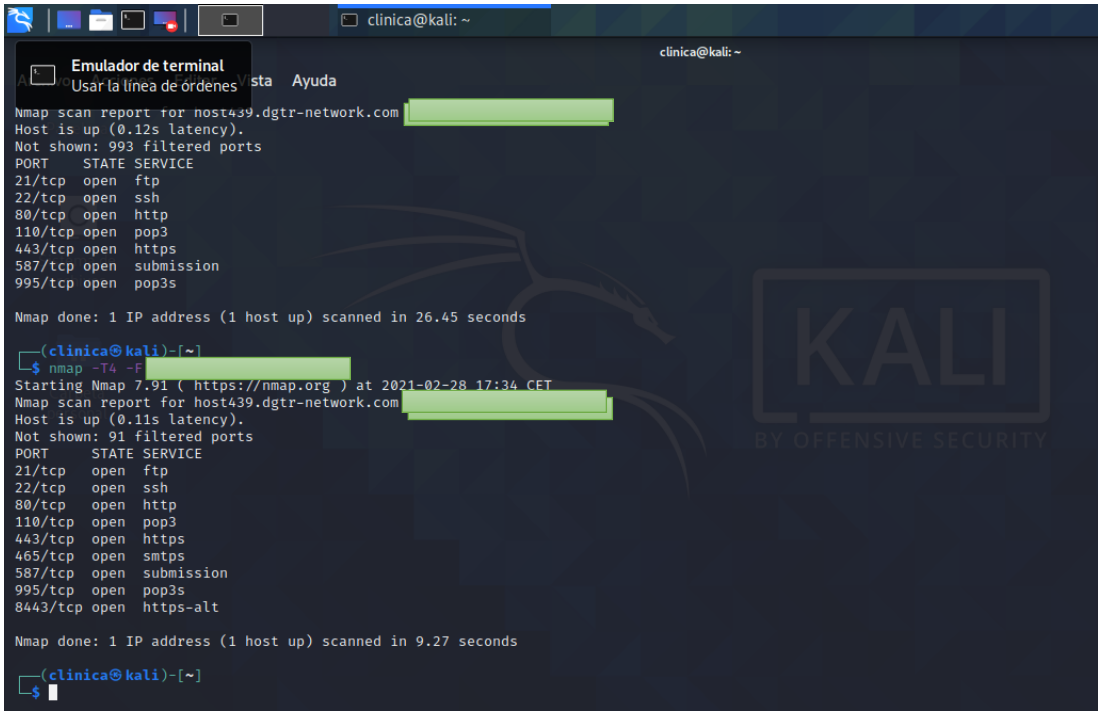
[16] ISO27000.ES, «El portal de ISO 27001. Gestión de la seguridad de la información,» 7 Diciembre 2016. [En línea]. Available: www.iso27000.es. [Último acceso: 20 Enero 2021].

ANEXOS

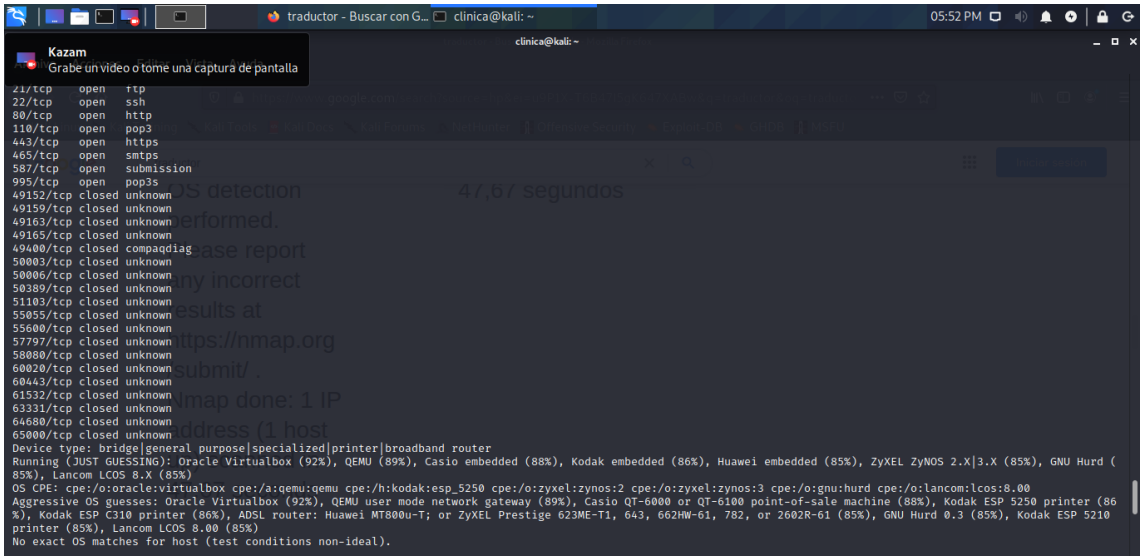
ANEXO 1: REPORTES DE LAS VULNERABILIDADES EN LA CLÍNICA

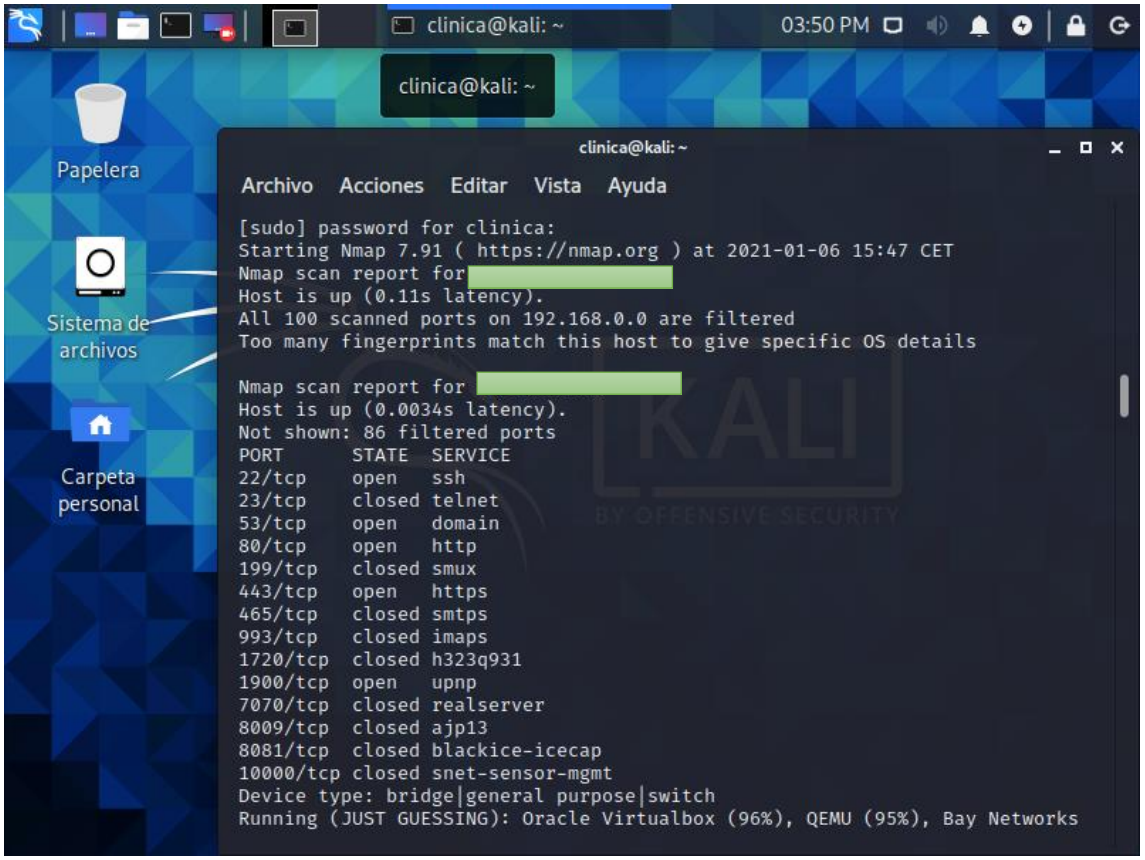
Las herramientas utilizadas para identificar las vulnerabilidades en el servidor web de la clínica fueron NMAP, NIKTO, OWASP ZAP bajo el sistema operativo virtual Kali Linux, estas son herramientas de libre distribución usadas en la seguridad informática como herramientas claves en la gestión de la información.

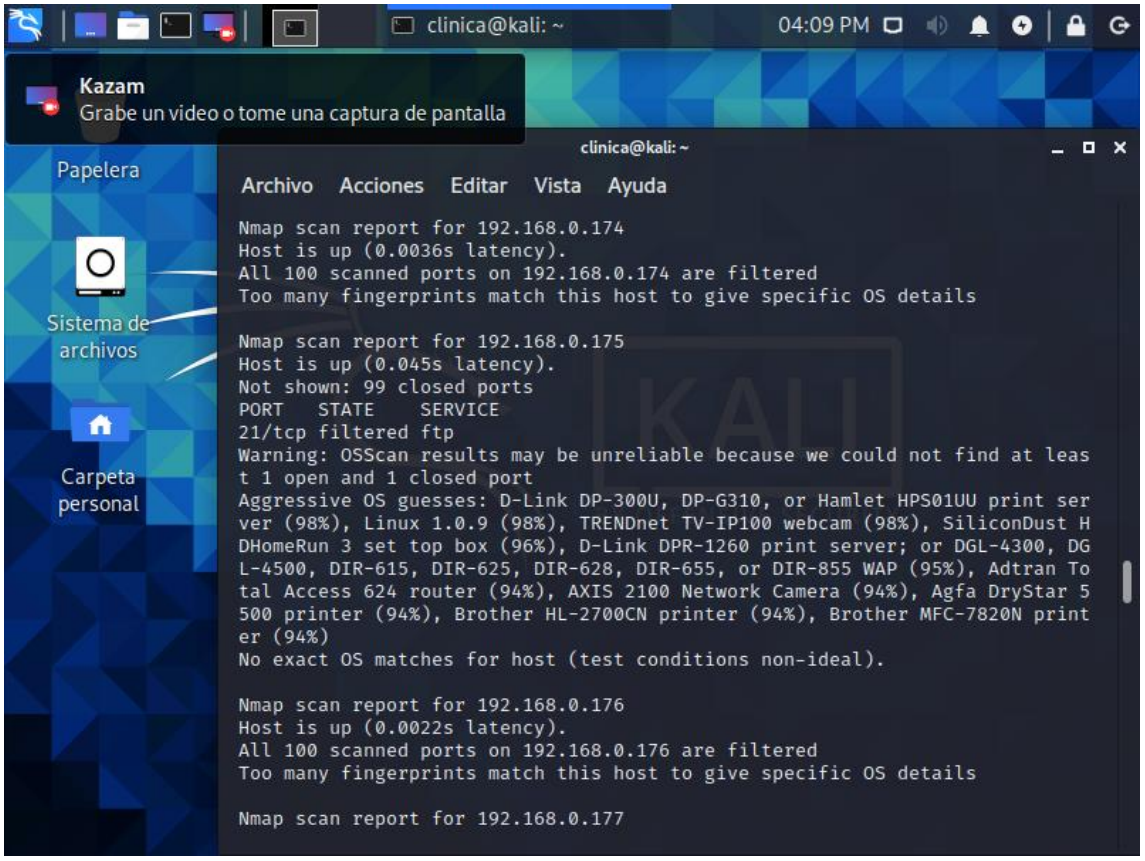
Como se observa en la imagen algunos de los puertos abiertos de la aplicación web de la clínica usando en comando NMAP seguido de la dirección IP 2[redacted] ó también usando el comando NMAP -T4 -F [redacted]2

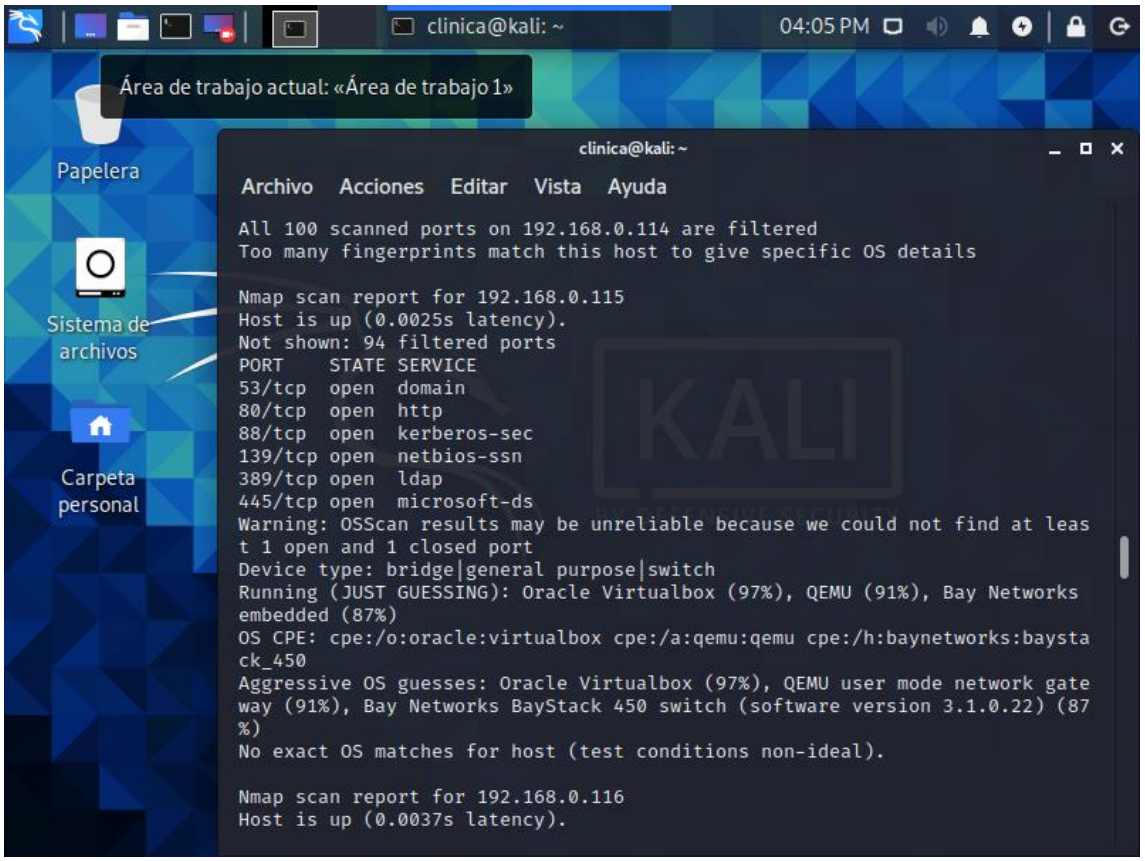


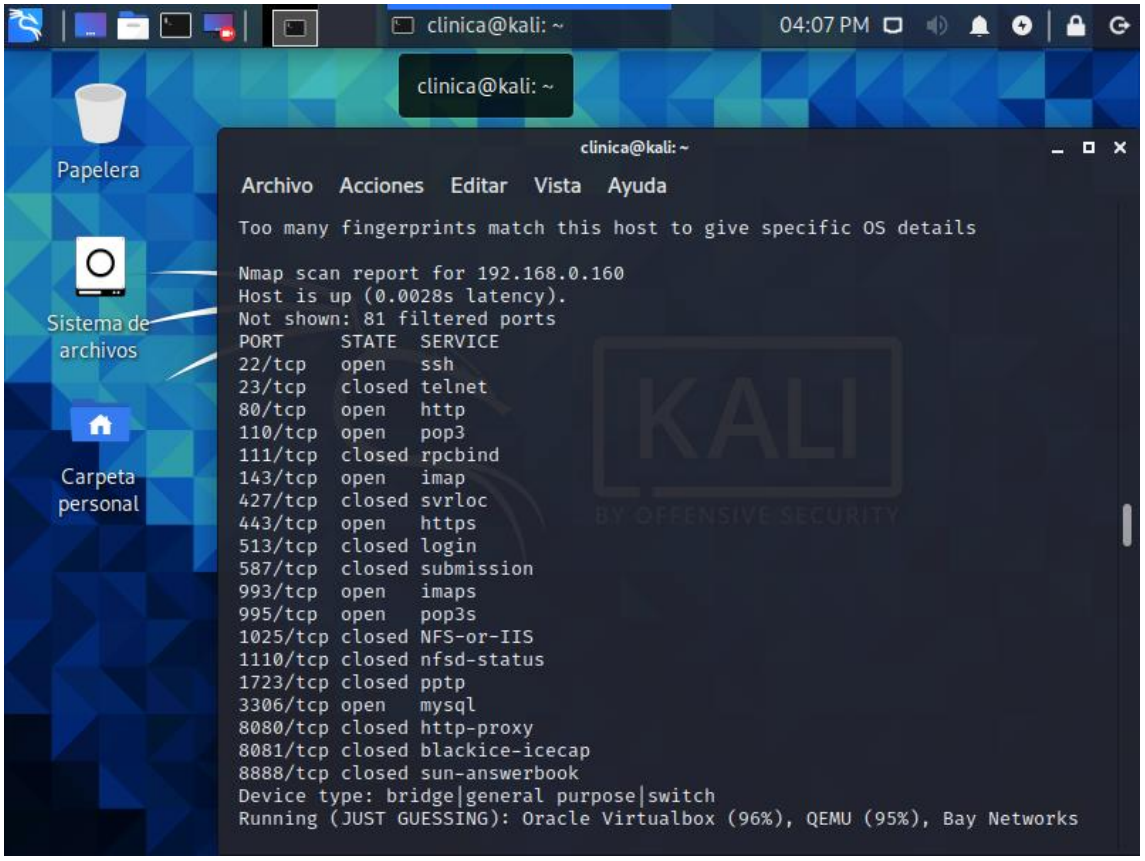
con el comando Sudo NMAP -0 [redacted]2, se detallan los activos de información que trabajan en el medio.

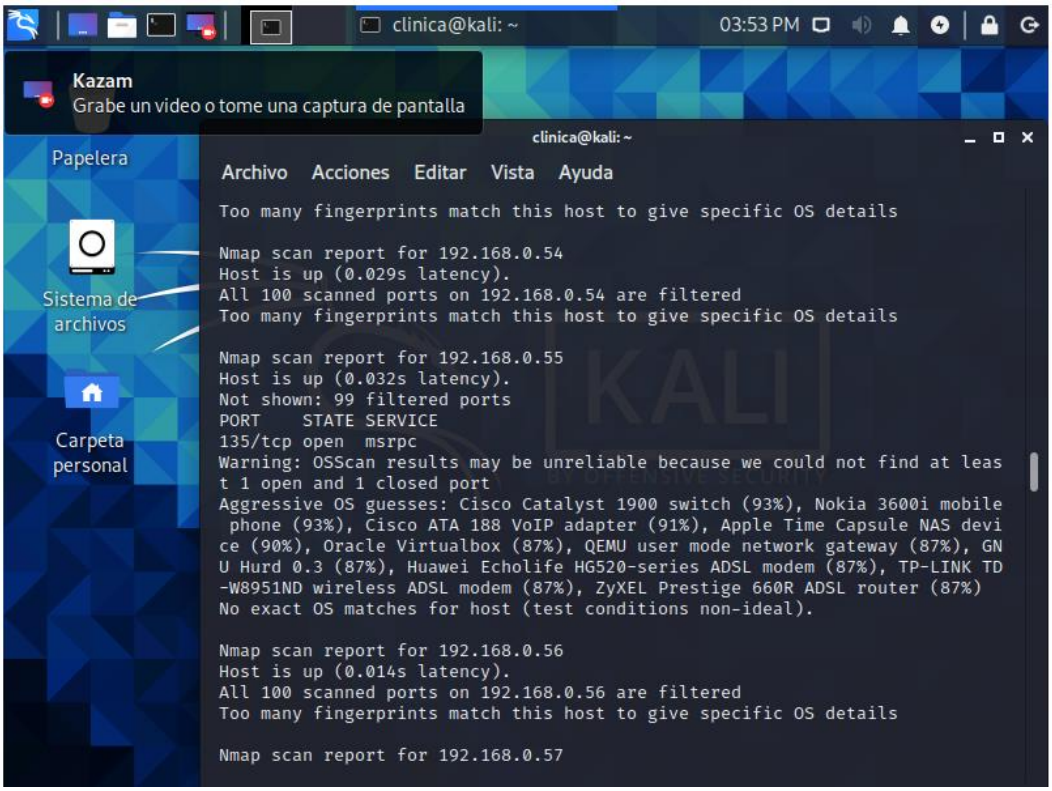

traductor - Buscar con G...
clinica@kali: ~
05:52 PM
Kazam
Graba un video o toma una captura de pantalla
21/tcp open ftp
22/tcp open ssh
80/tcp open http
110/tcp open pop3
443/tcp open https
465/tcp open smtps
587/tcp open submission
995/tcp open pop3s
49152/tcp closed unknown
49159/tcp closed unknown
49163/tcp closed unknown
49165/tcp closed unknown
49400/tcp closed compaqdiag
50003/tcp closed unknown
50006/tcp closed unknown
50389/tcp closed unknown
51103/tcp closed unknown
55055/tcp closed unknown
55600/tcp closed unknown
57797/tcp closed unknown
58080/tcp closed unknown
60020/tcp closed unknown
60443/tcp closed unknown
61532/tcp closed unknown
63331/tcp closed unknown
64680/tcp closed unknown
65000/tcp closed unknown
Device type: bridge|general purpose|specialized|printer|broadband router
Running (JUST GUESSING): Oracle Virtualbox (92%), QEMU (89%), Casio embedded (88%), Kodak embedded (86%), Huawei embedded (85%), ZyXEL ZyNOS 2.X|3.X (85%), GNU Hurd (85%), Lancom LCOS 8.X (85%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:kodak:esp_5250 cpe:/o:zyxel:zynos:2 cpe:/o:zyxel:zynos:3 cpe:/o:gnu:hurd cpe:/o:lancom:lcos:8.00
Aggressive OS guesses: Oracle Virtualbox (92%), QEMU user mode network gateway (89%), Casio QT-6000 or QT-6100 point-of-sale machine (88%), Kodak ESP 5250 printer (86%), Kodak ESP C310 printer (86%), ADSL router: Huawei MT800u-T; or ZyXEL Prestige 623ME-T1, 643, 662HW-61, 782, or 2602R-61 (85%), GNU Hurd 0.3 (85%), Kodak ESP 5210 printer (85%), Lancom LCOS 8.00 (85%)
No exact OS matches for host (test conditions non-ideal).


clinica@kali: ~
03:50 PM
clinica@kali: ~
Papelera
Sistema de archivos
Carpeta personal
clinica@kali: ~
Archivo Acciones Editar Vista Ayuda
[sudo] password for clinica:
Starting Nmap 7.91 (https://nmap.org) at 2021-01-06 15:47 CET
Nmap scan report for [redacted]
Host is up (0.11s latency).
All 100 scanned ports on 192.168.0.0 are filtered
Too many fingerprints match this host to give specific OS details
Nmap scan report for [redacted]
Host is up (0.0034s latency).
Not shown: 86 filtered ports
PORT STATE SERVICE
22/tcp open ssh
23/tcp closed telnet
53/tcp open domain
80/tcp open http
199/tcp closed smux
443/tcp open https
465/tcp closed smtps
993/tcp closed imaps
1720/tcp closed h323q931
1900/tcp open upnp
7070/tcp closed realserver
8009/tcp closed ajp13
8081/tcp closed blackice-icecap
10000/tcp closed snet-sensor-mgmt
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (95%), Bay Networks


clinica@kali: ~
04:09 PM
Kazam
Grabe un video o tome una captura de pantalla
Papelera
Sistema de archivos
Carpeta personal
clinica@kali: ~
Archivo Acciones Editar Vista Ayuda
Nmap scan report for 192.168.0.174
Host is up (0.0036s latency).
All 100 scanned ports on 192.168.0.174 are filtered
Too many fingerprints match this host to give specific OS details
Nmap scan report for 192.168.0.175
Host is up (0.045s latency).
Not shown: 99 closed ports
PORT STATE SERVICE
21/tcp filtered ftp
Warning: OSScan results may be unreliable because we could not find at leas
t 1 open and 1 closed port
Aggressive OS guesses: D-Link DP-300U, DP-G310, or Hamlet HPS01UU print ser
ver (98%), Linux 1.0.9 (98%), TRENDnet TV-IP100 webcam (98%), SiliconDust H
DHomeRun 3 set top box (96%), D-Link DPR-1260 print server; or DGL-4300, DG
L-4500, DIR-615, DIR-625, DIR-628, DIR-655, or DIR-855 WAP (95%), Adtran To
tal Access 624 router (94%), AXIS 2100 Network Camera (94%), Agfa DryStar 5
500 printer (94%), Brother HL-2700CN printer (94%), Brother MFC-7820N print
er (94%)
No exact OS matches for host (test conditions non-ideal).
Nmap scan report for 192.168.0.176
Host is up (0.0022s latency).
All 100 scanned ports on 192.168.0.176 are filtered
Too many fingerprints match this host to give specific OS details
Nmap scan report for 192.168.0.177

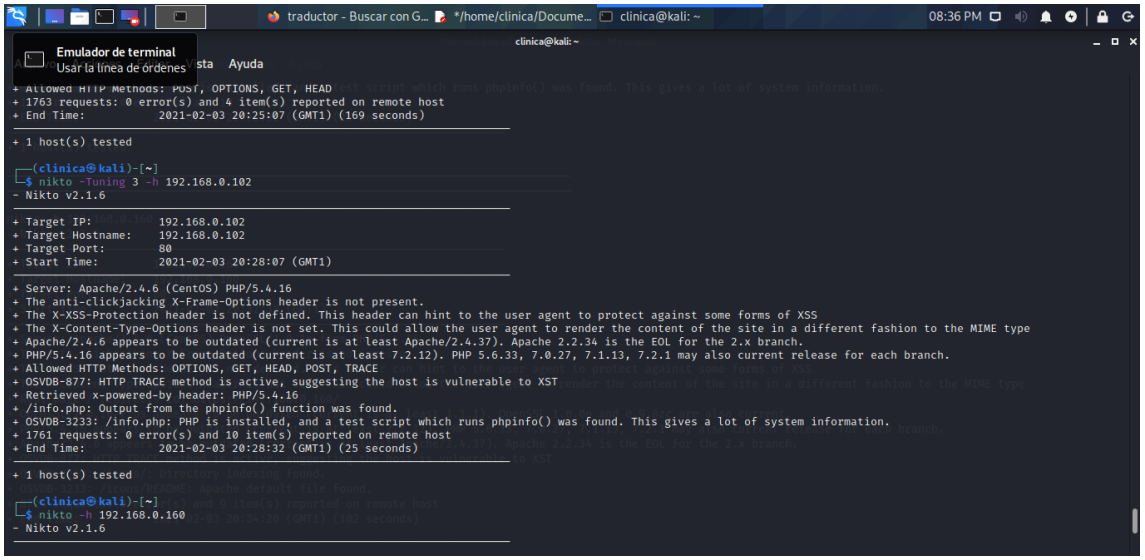

clinica@kali: ~
04:05 PM
Área de trabajo actual: «Área de trabajo 1»
Papelera
Sistema de archivos
Carpeta personal
clinica@kali: ~
Archivo Acciones Editar Vista Ayuda
All 100 scanned ports on 192.168.0.114 are filtered
Too many fingerprints match this host to give specific OS details
Nmap scan report for 192.168.0.115
Host is up (0.0025s latency).
Not shown: 94 filtered ports
PORT STATE SERVICE
53/tcp open domain
80/tcp open http
88/tcp open kerberos-sec
139/tcp open netbios-ssn
389/tcp open ldap
445/tcp open microsoft-ds
Warning: OSScan results may be unreliable because we could not find at leas
t 1 open and 1 closed port
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (97%), QEMU (91%), Bay Networks
embedded (87%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baysta
ck_450
Aggressive OS guesses: Oracle Virtualbox (97%), QEMU user mode network gate
way (91%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (87
%)
No exact OS matches for host (test conditions non-ideal).
Nmap scan report for 192.168.0.116
Host is up (0.0037s latency).

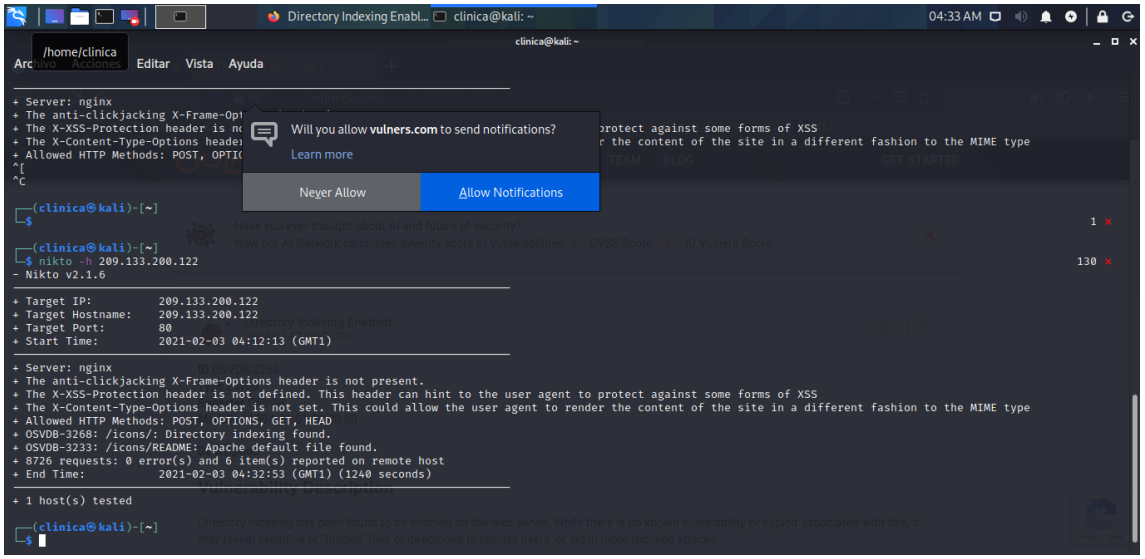

clinica@kali: ~
04:07 PM
clinica@kali: ~
Papelera
Sistema de archivos
Carpeta personal
clinica@kali: ~
Archivo Acciones Editar Vista Ayuda
Too many fingerprints match this host to give specific OS details
Nmap scan report for 192.168.0.160
Host is up (0.0028s latency).
Not shown: 81 filtered ports
PORT STATE SERVICE
22/tcp open ssh
23/tcp closed telnet
80/tcp open http
110/tcp open pop3
111/tcp closed rpcbind
143/tcp open imap
427/tcp closed svrloc
443/tcp open https
513/tcp closed login
587/tcp closed submission
993/tcp open imaps
995/tcp open pop3s
1025/tcp closed NFS-or-IIS
1110/tcp closed nfsd-status
1723/tcp closed pptp
3306/tcp open mysql
8080/tcp closed http-proxy
8081/tcp closed blackice-icecap
8888/tcp closed sun-answerbook
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (95%), Bay Networks


clinica@kali: ~
03:53 PM
Kazam
Grabe un video o tome una captura de pantalla
Papelera
Sistema de archivos
Carpeta personal
clinica@kali: ~
Archivo Acciones Editar Vista Ayuda
Too many fingerprints match this host to give specific OS details
Nmap scan report for 192.168.0.54
Host is up (0.029s latency).
All 100 scanned ports on 192.168.0.54 are filtered
Too many fingerprints match this host to give specific OS details
Nmap scan report for 192.168.0.55
Host is up (0.032s latency).
Not shown: 99 filtered ports
PORT STATE SERVICE
135/tcp open msrpc
Warning: OSScan results may be unreliable because we could not find at leas
t 1 open and 1 closed port
Aggressive OS guesses: Cisco Catalyst 1900 switch (93%), Nokia 3600i mobile
phone (93%), Cisco ATA 188 VoIP adapter (91%), Apple Time Capsule NAS devi
ce (90%), Oracle Virtualbox (87%), QEMU user mode network gateway (87%), GN
U Hurd 0.3 (87%), Huawei Echolife HG520-series ADSL modem (87%), TP-LINK TD
-W8951ND wireless ADSL modem (87%), ZyXEL Prestige 660R ADSL router (87%)
No exact OS matches for host (test conditions non-ideal).
Nmap scan report for 192.168.0.56
Host is up (0.014s latency).
All 100 scanned ports on 192.168.0.56 are filtered
Too many fingerprints match this host to give specific OS details
Nmap scan report for 192.168.0.57

NIKTO

A través del comando Nikto -h podemos observamos las vulnerabilidades en el servidor web:

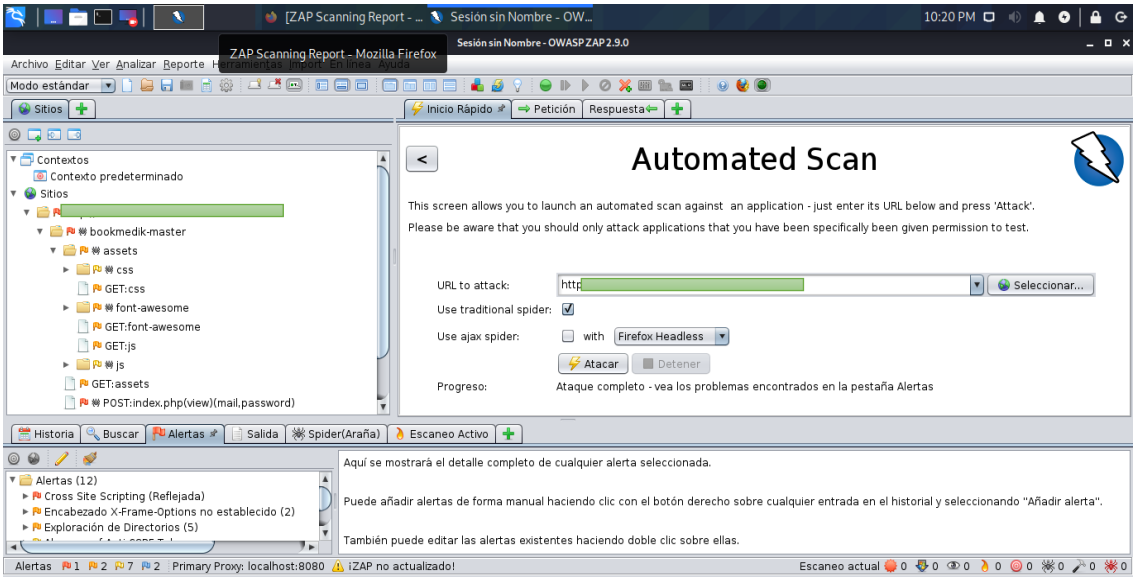




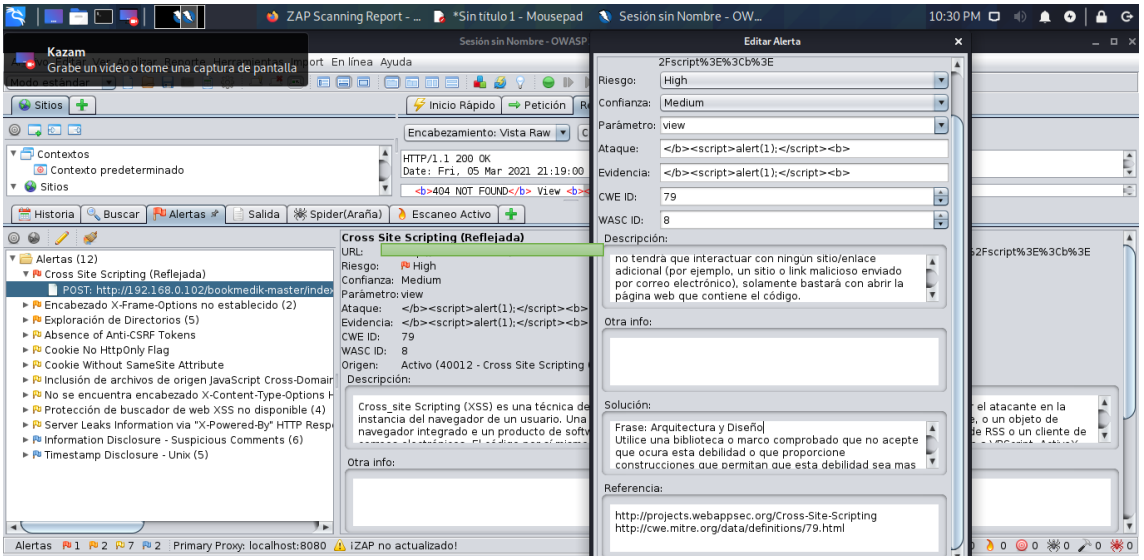
OWASP ZAP

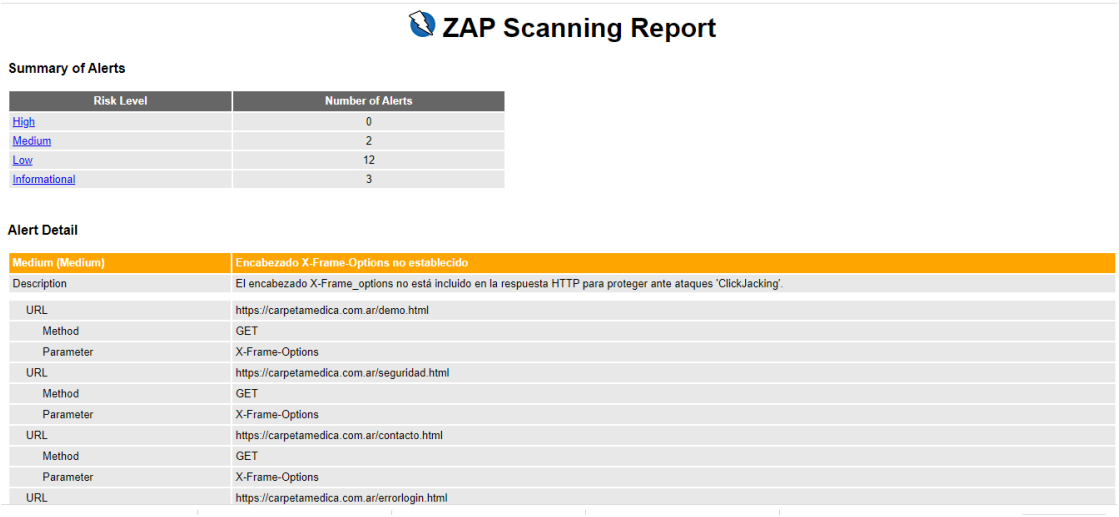
El ataque por parte de OWASP ZAP que permite la búsqueda de vulnerabilidades automáticas, funciona de la siguiente forma:

- Se hace un recorrido de URL del servidor de la clínica [redacted] con el Spider
- Se realiza un escaneo activo de la aplicación web en el spider
- Se analiza el contenido de la aplicación web y se muestran las alertas en este caso son 12, en función de la criticidad de la vulnerabilidad.



Este panel donde se muestra las posibles vulnerabilidades y el riesgo que conlleva, muestra, además, información sobre cómo se puede vulnerar, y qué medidas se pueden tomar para evitar que dicho fallo de seguridad sea vulnerable





ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	12
Informational	3

Alert Detail

Medium (Medium)	Encabezado X-Frame-Options no establecido
Description	El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'.
URL	https://carpetamedica.com.ar/demo.html
Method	GET
Parameter	X-Frame-Options
URL	https://carpetamedica.com.ar/seguridad.html
Method	GET
Parameter	X-Frame-Options
URL	https://carpetamedica.com.ar/contacto.html
Method	GET
Parameter	X-Frame-Options
URL	https://carpetamedica.com.ar/errorlogin.html

ANEXO 2: TABLA DE EVALUACIÓN DE LAS AMENAZAS

AMENAZA	DESCRIPCIÓN DE LA AMENAZA	AGENTE DE AMENAZA
1013	Código malicioso	Hacker
1029	Modificación no autorizada de información	Empleado sin experiencia
1028	Modificación no autorizada de información	Personal descontento
1031	Modificación no autorizada de información	Ex-empleado
1041	Virus en las redes o computadoras	Hacker
1042	Virus en las redes o computadoras	Personal descontento
1048	UPS defectuoso o sin mantenimiento	Personal descontento
1043	Virus en las redes o computadoras	Personal interno inexperto (accidental)
1025	Acceso no autorizado	Personal interno inexperto (accidental)
1024	Acceso no autorizado	Personal interno descontento (intencional)
1044	Fallas de hardware en los equipos	Material (falla)

ALERTA	DIRECCIÓN DE URL ESCANEADA	RIESGO	PARÁMETRO	ATAQUE	EVIDENCIA	DESCRIPCIÓN	SOLUCIÓN
CroosSite Scripting (Reflejada)	http://192.168.0.102/bookmedik-master/index.php?view=%3C%2Fb%3E%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E%3Cb%3E	Alto	Vista	<script>alert(1):</script>	<script>alert(1):</script>	objetivos preferidos de los atacantes incluyen mensajes en carteleras de anuncios, mensajes de correo electrónico y programas de chat. Robar información	Cualquier comprobación de seguridad que se vaya a realizar en el lado del cliente, asegúrese de que estas comprobaciones se encuentren duplicadas en el lado del servidor, para evitar el CWE-602. Los atacantes pueden eludir las comprobaciones del lado del cliente modificando los valores después de que se hayan realizado las comprobaciones, o cambiando al cliente para poder eliminar de forma completa las comprobaciones del lado del cliente. Después, estos valores que fueron modificados serán enviados al servidor.

Encabezado X-Frame-Options no establecido		Medio	X-Frame-Options			El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'.	Los navegadores de web más modernos apoyan la cabecera HTTP X-Frame-Options. Asegúrese que está establecido en todas las páginas web devuelta por su sitio (si usted espera que la página este enmarcada solo por páginas en su servidor
Exploración de Directorios		Medio		Parent Directory		Es posible ver el listado de directorios. La lista de directorios puede revelar scripts ocultos, incluyen archivos, copia de seguridad de los archivos de origen, etc, que se pueden acceder para leer información sensible.	Desactivar la exploración de directorios. Si esto es necesario, asegúrese de que los archivos de la lista no inducen riesgos.

Absence of Anti-CSRF Tokens		Bajo		<form accept-charset="UTF-8" role="form" method="post" action="index.php?view=processlogin">		Una solicutud falsa entre sitios en un ataque que compromete y obliga a una víctima a enviar su solicitud HTTP a un destino objetivo sin su conocimiento o intención para poder realizar una acción como víctima.	Asegúrese de que su aplicación esté libre de fallas de secuencias de comandos entre sitios, ya que la mayoría de las defensas de CSRF pueden detenerse por alto por medio del uso de secuencias de comandos manejadas por el atacante.

Cookie No HttpOnly Flag		Bajo	PHP SESSID	Set-cookie: PHPSESSID		Se ha establecido una cookie sin la bandera HttpOnly, lo que significa que la cookie puede ser accedida mediante JavaScript. Si un script malicioso puede ser ejecutado en esta página entonces la cookie será accesible y podrá ser transmitida a otro sitio. Si esta es una cookie de sesión entonces el secuestro de sesión podría ser posible.	Asegúrese que la bandera HttpOnly está establecida para todas las cookies.

Cookie Without SameSite Attribute		Bajo	PHP SESSID	Set-cookie: PHPSESSID		Se ha establecido una cookie sin el atributo SameSite, lo que significa que la cookie se puede enviar como resultado de una solicitud 'entre sitios'. El atributo SameSite es un contra medida para la falsificación de solicitudes entre sitios, la inclusión de scripts entre sitios y los ataques de tiempo efectivo	Asegúrese de que el atributo SameSite esté configurado como 'laxo' o idealmente 'estricto' para todas las cookies.
Inclusión de archivos de origen JavaScript Cross-Domain		Bajo	https://maps.googlesapis.com/maps/api/js		https://maps.googlesapis.com/maps/api/js>< script>	Las páginas incluyen uno o más archivos encriptados de un dominio de terceros	Asegúrese que los archivos de la fuente JavaScript están descargados solo de sus fuentes confiables, y las fuentes no pueden ser controladas por los usuarios finales de la aplicación.

No se encuentra encabezado X-Content-Type-Options Header		Bajo	x-Content-Type-Option			El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado.	Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing.
Protección de buscador de web XSS no disponible		Bajo	X-XSS-PROTECTION			La protección del buscador de web XSS no está disponible, o está deshabilitada por la configuración de la cabecera de respuesta de HTTP 'X-XSS-Protection' en el	Asegúrese que el filtro XSS del navegador web está habilitado, estableciendo el encabezado de respuesta HTTP X-XSS-Protection en '1'

						servidor de web	
El servidor filtra información a través de los campos de encabezado de respuesta HTTP "X-Powered-By"		Bajo			X-Powered-By: PHP/5.4.16	El servidor web / de aplicaciones está filtrando información a través de uno o más encabezados de respuesta HTTP "X-Powered-By". Acceso a dicha información puede facilitar a los atacantes la identificación de otros marcos / componentes de los que depende su aplicación web y las vulnerabilidades a las que dichos componentes pueden estar sujetos.	Asegúrese de que su servidor web, servidor de aplicaciones, equilibrador de carga, etc. esté configurado para suprimir los encabezados "X-Powered-By".
Divulgación de información: comentario		Bajo				La respuesta parece contener comentarios sospechosos que pueden ayudar a un atacante.	Elimine todos los comentarios que devuelvan información que pueda ayudar a un atacante y solucione cualquier problema subyacente al que se refiera.

s sospechos os							
Divulgació n de marca de tiempo – Unix		Bajo			4285714 3	La aplicación / servidor web reveló una marca de tiempo – Unix	Confirme manualmente que los datos de la marca de tiempo no son confidenciales y que los datos no se pueden agregar para revelar patrones explotables.

ANEXO 3: MATRIZ DE ACTIVOS DE INFORMACIÓN DEL PROCESO DE CITAS CLINICAS

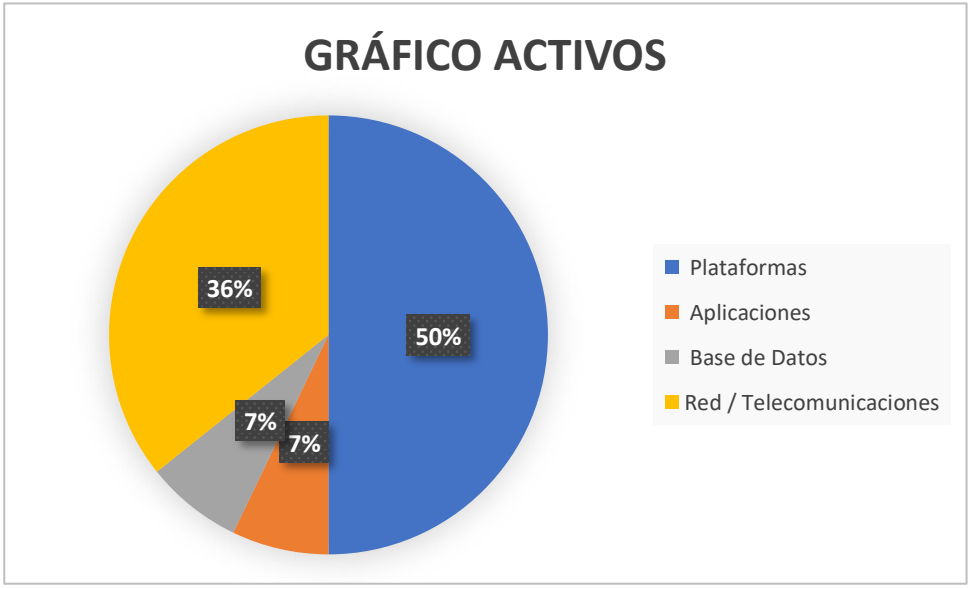
Id	Activo	Descripción	Clasificación (Criterio / No Criterio)	Funcionario Responsable	Funcionario que resguarda
Sis-ser003	SERVIDOR DELL POWEREDGE T140 SERVICE TAG: 7D4JBZ2	Servidor principal que contiene los servidores secundarios y demás equipos	Crítico	Departamento Tic	Jefe de Departamento de Tecnologías de la información y Comunicación
Sis-ser004	SERVIDOR WEB MYSQL	Aplicativos WEB de la clínica.	Crítico	Personal de desarrollo Semi Senior	Jefe de Departamento de Tecnologías de la información y Comunicación
Sis-ser005	SERVIDOR DE BD SQLSERVER	Servidor que contiene los datos módulos de citas, consultas, historial médico, usuarios, etc.	Crítico	Personal de desarrollo Semi Senior	Jefe de Departamento de Tecnologías de la información y Comunicación
Sis-ser006	SERVIDOR DE SERVICIOS PROMOX	Servidor de virtualización de maquinas	Crítico	Administrador de redes	Jefe de Departamento de Tecnologías de la información y Comunicación

Sis-ser007	SERVIDOR DE IMPRESIÓN HAMLET HPS01UU PRINT SERVER	Impresiones de forma remota en los diferentes departamentos en la clínica	No crítico	Administrador de redes	Jefe de Departamento de Tecnologías de la información y Comunicación
Rec-067	RELOJ BIOMÉTRICOS DE ACCESO – ZTECO	Control de asistencia del personal	No crítico	Administrador de redes	Jefe de Departamento de Tecnologías de la información y Comunicación
Rec-066	SWITCH TP-LINK TL-SG3428	SWITH principal para la Conexión con los dispositivos de la clínica PC, portátil, Router, otro Switch, etc	No crítico	Administrador de redes	Jefe de Departamento de Tecnologías de la información y Comunicación
Rec-067	SWITCH GIGABIT TP-LINK TL-SG1048	Conexión de equipos a la red de la clínica	No crítico	Administrador de redes	Jefe de Departamento de Tecnologías de la información y Comunicación
Rec-035	ROUTER HUAWEI PROVEEDOR NETLIFE	Servicio de Internet 100MB	No crítico	Administrador de redes	Jefe de Departamento de Tecnologías de la información y Comunicación
Rec-023	TELEFONO COMUTADOR PANASONIC KX-T7730	Monitoreo de llamadas internas automáticas	No crítico	Administrador de redes	Jefe de Departamento de Tecnologías de la información y Comunicación
Rec-001	ROUTER TP-LINK	Dispositivo de red para conexión a internet	No crítico	Administrador de redes	Jefe de Departamento de Tecnologías de la información y Comunicación

Sis-ser009	SERVIDOR DE IMPRESIÓN DP-G310	Impresiones de forma remota en los diferentes departamentos en la clínica	No crítico	Administrador de redes	Jefe de Departamento de Tecnologías de la información y Comunicación
Sis-act001	CAMARA DE VIGILANCIA TRENDNET TV-IP100 WEBCAM	Control del trabajo y actividad de los empleados	No crítico	Administrador de redes	Jefe de Departamento de Tecnologías de la información y Comunicación
Rec-069	BAY NETWORKS BAYSTACK 450 SWITCH	Conexión de equipos a la red de la clínica	No crítico	Administrador de redes	Jefe de Departamento de Tecnologías de la información y Comunicación

Para el análisis en el Departamento Administrativo de las TIC de la clínica se tuvo en cuenta 14 activos, los cuales se encuentra clasificados de la siguiente manera: Plataforma 50%, Aplicaciones 7%, Base de Datos 7%, Red / Telecomunicaciones 36%.

	CATEGORIA ACTIVO	CANTIDAD
1	Plataformas	7
2	Aplicaciones	1
3	Base de Datos	1
4	Red / Telecomunicaciones	5
		14



ANEXO 4: MATRIZ DE EVALUACIÓN DE AMENAZAS DE LOS ACTIVOS DE INFORMACIÓN EN EL PROCESO DE CITAS DE LACLINICA

Listado de amenazas según Norma ISO 27002, para el análisis de los activos de información en el proceso de citas.

Equipos	**Amenaza**	**Agente de la Amenaza**
Servidor Web	Código malicioso	Hacker
	Modificación no autorizada de información	Personal interno inexperto (accidental) Personal interno descontento (intencional) Ex–empleado
	Virus en las redes o computadoras	Hacker
Servidor de Base de Datos	Código malicioso	Hacker
	Modificación no autorizada de información	Personal interno inexperto (accidental) Personal interno descontento (intencional) Ex–empleado
	Virus en las redes o computadoras	Hacker
Router	Virus en las redes o computadoras	Hacker
	Modificación no autorizada de información	Personal interno descontento (intencional)
Switch	Modificación no autorizada de información	Personal interno inexperto (accidental) Personal interno descontento (intencional) Ex–empleado
Servidor de impresión	UPS defectuoso o sin mantenimiento	Personal interno descontento (intencional)
	Fallas de hardware en los equipos	Material (falla)

A partir de los 14 activos identificados, se recopilaron 22 amenazas que pueden generar un impacto negativo para en la clínica, dichas amenazas se encuentra clasificadas de la siguiente manera: código malicioso hacker 14%, modificación no autorizada de información - personal interno inexperto accidental 14%, modificación no autorizada de información -exempleado 18%, virus de computadoras - hacker 9%, modificación no autorizada de información - personal interno descontento intencional 23%, ups defectuoso o sin mantenimiento - personal interno descontento intencional 4%, fraude 4%, acceso no autorizado 9% y fallas de hardware en los equipos 5%

ID	CATEGORIA AMENAZA	AGENTE DE AMENAZA	CANTIDAD
1013	CÓDIGO MALICIOSO	HACKER	3
1029	MODIFICACIÓN NO AUTORIDADA DE INFORMACIÓN	PERSONAL INTERNO INEXPERTO ACCIDENTAL	3
1031	MODIFICACIÓN NO AUTORIDADA DE INFORMACIÓN	EX-EMPLEADO	4
1041	VIRUS DE COMPUTADORA	HACKER	2
1028	MODIFICACIÓN NO AUTORIDADA DE INFORMACIÓN	PERSONAL INTERNO DESCONTENTO INTENCIONAL	5
1048	UPS DEFECTUOSO O SIN MANTENIMIENTO	PERSONAL INTERNO DESCONTENTO INTENCIONAL	1
1015	FRAUDE	PERSONAL INTERNO DESCONTENTO INTENCIONAL	1
1025	ACCESO NO AUTORIZADO	PERSONAL INTERNO INEXPERTO ACCIDENTAL	2
1044	LLAS DE HARDWARE EN LOS EQUIP	MATERIAL FALLA	1
			22

ANEXO 5: MATRIZ DE ANÁLISIS DE AMENAZAS PARA EL SISTEMA DE LA CLÍNICA.

A continuación, se presentan el registro parcial de la plantilla correspondiente análisis de amenazas, donde se identifica algunas medidas de estrategias tomadas para el riesgo de la amenaza.

ID Amenaza	Descripción de la amenaza	Agente de amenaza	Activo	Descripción del Activo	Control	Estrategia	Controles Propuestos
1013	Código malicioso	Hacker	Sis-ser004	SERVIDOR WEB MYSQL	A.5.1.1 Políticas para la seguridad de la información A.14.2.6 Ambiente de desarrollo seguro	Mitigar	Antivirus que incluyan actualización automática para la detención, prevención y controles de recuperación para proteger contra código malicioso, configurar contraseñas de alta seguridad, Instalar las últimas versiones de los parches disponibles para el software, servicios de los equipos operativos, cambiar contraseñas de administrador.
			Sis-ser005	SERVIDOR DE BD SQLSERVER	A.12.2.1 Controles contra códigos maliciosos	Mitigar	Antivirus que incluyan actualización automática para la detención, prevención y controles de recuperación para proteger contra código malicioso, Configurar

							contraseñas de alta seguridad, Instalar las últimas versiones de los parches disponibles para el software, servicios de los equipos operativos, cambiar contraseñas de administrador.
			Rec-001	ROUTER TP-LINK	A.9.2.5 Revisión de los derechos de acceso de usuarios	Mitigar	Antivirus que incluyan actualización automática para la detención, prevención y controles de recuperación para proteger contra código malicioso, Configurar contraseñas de alta seguridad, Instalar las últimas versiones de los parches disponibles para el

							software, servicios de los equipos operativos, cambiar contraseñas de administrador.
1029	Modificación no autorizada de información	Personal interno inexperto (accidental)	Sis-ser004	SERVIDOR WEB MYSQL	A.9.4.1 Restricción de acceso a la información	Mitigar	Permiso para el acceso a la web, información solo para personal autorizado, Capacitación, respaldos de los datos de la clínica.
			Sis-ser005	SERVIDOR DE BD SQLSERVER	A.9.4.2 Procedimiento de ingreso seguro	Mitigar	Permiso para el acceso a la web, información solo para personal autorizado, Capacitación, respaldos de los datos de la clínica.
			Sis-ser100	SWITCH GIGABIT TP-LINK TL-SG1048	A.9.4.1 Restricción de acceso a la información	Mitigar	Sistema prevención a intrusos, restricción a acceso a la información solo personal autorizados, respaldo de datos
1031	Modificación no autorizada de información	Ex–empleado	Sis-ser005	SERVIDOR DE BD SQLSERVER	A.9.2.2 Suministro de acceso de usuarios A.9.2.6 Retiro o ajuste de los derechos de acceso	Mitigar	Eliminación de accesos a la información cuando el empleado finaliza su contrato, respaldo de los datos.

			Rec-067	SWITCH GIGABIT TP-LINK TL-SG1048	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información	Mitigar	Sistema de prevención a intrusos, Eliminación de acceso a la información a exempleados
			Sis-ser005	SERVIDOR DE BD SQLSERVER	A.18.2.1 Revisión independiente de la seguridad de la información	Mitigar	Restricción a la información, respaldo de la información, sistema prevención a intrusos, eliminación acceso a la información a exempleados, cambios de contraseña de administrador
			Sis-ser004	SERVIDOR WEB MYSQL	A.7.1.2 Términos y condiciones del Empleo	Mitigar	Restricción a la información, respaldo de la información, sistema prevención a intrusos, eliminación acceso a la información a exempleados, cambios de contraseñas de administrador
1041	Virus en las redes o computadoras	Hacker	Sis-ser005	SERVIDOR DE BD SQLSERVER	A.8.3.1 Gestión de medios removibles	Mitigar	Cambio de contraseñas de nuestros sistemas, Antivirus que incluyan actualización automática para la detención, prevención y controles de recuperación, actualizar los sistemas operativos, y todos los equipos conectados al ordenador

			Rec-001	ROUTER TP-LINK	A.12.2.1 Controles contra códigos maliciosos	Mitigar	Cambio de contraseñas de nuestros sistemas, actualizar el firmware del router o todo equipo conectado al ordenador
1028	Modificación no autorizada de información	Personal interno descontento (intencional)	Rec-067	SWITCH GIGABIT	A.9.2.5 Revisión de los derechos de acceso de usuarios	Mitigar	Sistema de prevención a intrusos, Permisos de acceso a usuarios
				TP-LINK TL-SG1048			
			Rec-001	ROUTER TP-LINK	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información	Mitigar	Sistema prevención a intrusos, contratos sobre acuerdos de servicios
			Rec-069	BAY NETWORKS BAYSTACK 450 SWITCH	A.9.2.1 Registro y cancelación de usuarios	Mitigar	Sistema prevención a intrusos, restricción a acceso a la información solo personal autorizados, respaldo de datos

			Sis-ser005	SERVIDOR DE BD SQLSERVER		Mitigar	Restricción a la información, respaldo de la información, cambios de contraseña de administrador
1048	UPS defectuoso o sin mantenimiento	Personal interno descontento (intencional)	Sis-ser006	SERVIDOR DE IMPRESIÓN DP-G310	A.11.2.4 Mantenimiento de equipos	Mitigar	Diseño eléctrico de un centro de datos admite una mayor eficiencia energética, respaldos de datos.
1015	Fraude	Personal interno descontento (intencional)	Sis-ser005	SERVIDOR DE BD SQLSERVER	A.12.7 Controles de auditorías de sistemas de información	Mitigar	Ingreso de claves robustas, Control de acceso BD, respaldos de información externos y nube.
1025	Acceso no autorizado	Personal interno inexperto (accidental)	Rec-069	BAY NETWORKS BAYSTACK 450 SWITCH	A.9.1.1 Política de control de acceso	Mitigar	Permiso de accesos a usuarios, actualización de antivirus y firewall, asignación de una red privada.
			Rec-066	SWITCH TP-LINK TL-SG3428	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información	Mitigar	Permiso de accesos a usuarios, actualización de antivirus y firewall, asignación de una red privada.

1044	Fallas de hardware en los equipos	Material (falla)	Sis-ser009	SERVIDOR DE IMPRESIÓN DP-G310	A.14.2.5 Principios de construcción de los sistemas seguros	Mitigar	configuración de permisos de accesos de nuestros empleados, Mantenimiento regulares a los diferentes dispositivos

ANEXO 6: PLAN DE ACCIÓN QUE DEFINA CONTROLES BASADOS EN LA NORMA ISO 27002

Se presenta un cuadro donde se indican algunos de los controles seleccionados de la Norma, en los riesgos mitigados según la amenazas.

Plan de acción y controles ISO 27002:2013							
Control	**Riesgo mitigado**	**Descripción**	**Responsables**	**Presupuesto estimado**	**Tiempo**	**INICIO**	**FIN**
A.5.1.1 Políticas para la seguridad de la información	Todos los riesgos	La institución definirá un conjunto de políticas para la seguridad de la información, aprobada por el Gerente, publicada y comunicada a los colaboradores y a las partes externas pertinentes.	Director de Tecnologías de la Información y Comunicación	-	4 meses	18-dic-2020	18-mar-2021
A.7.1.2 Términos y condiciones del Empleo	Modificación no autorizada de información Acceso no autorizado	Control de los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información	Director de Tecnologías de la Información y Comunicación		Implementado		

A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información	Modificación no autorizada de información Respaldos defectuosos	Los empleados de la clínica, recibirán capacitaciones sobre la conciencia y actualización de las políticas y procedimiento de la organización. Que sean relevantes para la función laboral.	Director de Tecnologías de la Información y Comunicación	8.000,00	6 meses	18-abr-2021	18-sep-2021
A.8.3.1 Gestión de medios removibles	Código malicioso Virus en las redes o computadoras	Definir y aprobar procedimientos para la gestión y uso de medios extraíbles, tales como: memorias USB, discos duros externos, CD.	Director de Tecnologías de la Información y Comunicación	-	Implementado		
A.9.1.1 Política de control de acceso	Código malicioso Modificación no autorizada de información Acceso no autorizado	Establecer, almacenar, revisará una política de control de acceso de usuarios basado en los privilegios de seguridad de la institución	Director de Tecnologías de la Información y Comunicación	-	Implementado		
A.9.1.2 Acceso a redes y a servicios en red	Modificación no autorizada de información	Se debe permitir el acceso a la red institucional únicamente a los usuarios autorizados conforme a las políticas de control de acceso.	Director de Tecnologías de la Información y Comunicación Todas las áreas	-	Implementado		

A.9.2.1 Registro y cancelación de usuarios	Código malicioso Modificación no autorizada de información	Permitir la asignación de derechos de acceso a usuarios para la administración.	Director de Tecnologías de la Información y Comunicación	-	3 meses	18-jul-2021	18-sep-2021
A.9.2.2 Suministro de acceso de usuarios	Código malicioso Modificación no autorizada de información	Proceso formal de provisión de acceso a los usuarios para asignar derechos de accesos para todos los tipos de usuarios a sistemas y servidores.	Director de Tecnologías de la Información y Comunicación	-		18-jul-2021	18-sep-2021
A.9.2.5 Revisión de los derechos de acceso de usuarios	Código malicioso Modificación no autorizada de información	Definir y aprobar un procedimiento para la revisión periódica de los derechos de acceso de usuarios por parte de los propietarios de los activos de información.	Director de Tecnologías de la Información y Comunicación	-	2 meses	18-nov-2021	18-dic-2021
A.9.2.6 Retiro o ajuste de los derechos de acceso	Código malicioso Modificación no autorizada de información	Definir y aprobar un procedimiento para la revocación de derechos de acceso de los usuarios al terminar su empleo o vinculación con la institución.	Director de Tecnologías de la Información y Comunicación	-	2 meses	18-jun-2021	18-jul-2021

A.9.3.1 Uso de información de autenticación secreta	Código malicioso Modificación no autorizada de información	Los usuarios deben cumplir políticas de contraseñas en la clínica, que son aplicadas en el sistema	Director de Tecnologías de la Información y Comunicación	-	5 meses	18-oct-2021	18-feb-2022
A.9.4.1 Restricción de acceso a la información	Código malicioso Modificación no autorizada de información	Se refiere al estándar de contraseña y autentificación	Director de Tecnologías de la Información y Comunicación	-	2 meses	18-may-2020	18-jun-2021
A.9.4.2 Procedimiento de ingreso seguro	Código malicioso Modificación no autorizada de información	Se debe solicitar usuario y contraseña al ingresar a los sistemas y aplicaciones.	Director de Tecnologías de la Información y Comunicación	-	3 semanas	18-jul-2021	08-ago-2021
A.9.4.5 Control de acceso a códigos fuente de programas	Modificación no autorizada de información	El acceso al código fuente de los programas debe ser restringido únicamente a usuarios autorizados.	Director de Tecnologías de la Información y Comunicación	-	Implementado		
A.10.1.1 Política sobre el uso de controles criptográficos	Código malicioso	Definir y aprobar una política para el uso de controles criptográficos, tales como: certificados digitales, cifrado de claves, etc.	Director de Tecnologías de la Información y Comunicación	1.000,00	3 meses	18-oct-2021	18-dic-2021

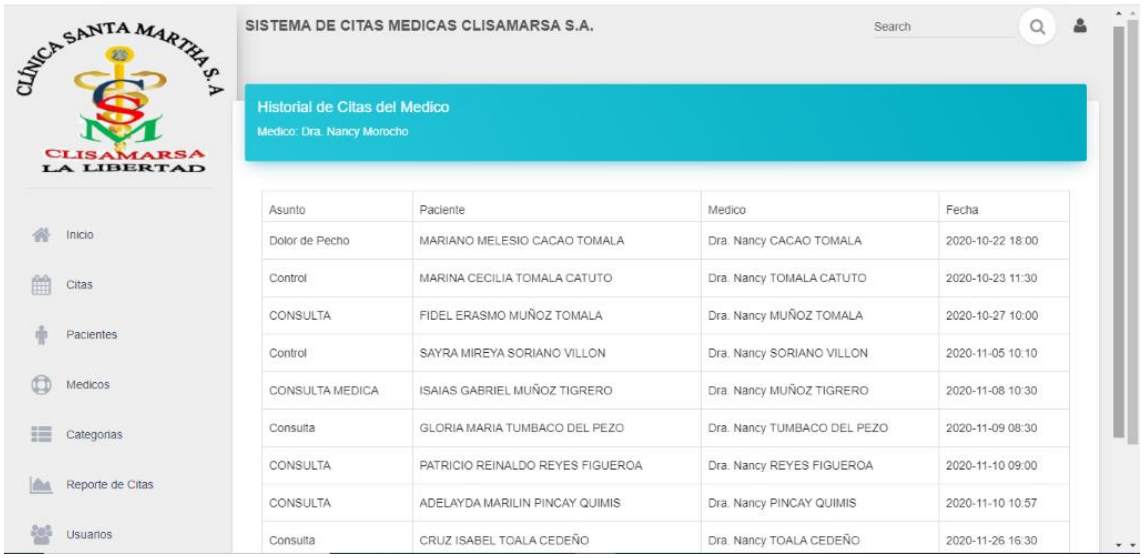
A.11.1.2 Controles de acceso físico	Modificación no autorizada de información Negación de servicio	Implementación de controles de acceso y protección física, tales como: acceso biométrico, puerta de acero, ascensor, cámaras de seguridad al interior y exterior, alertas	Director de Tecnologías de la Información y Comunicación	.	Implementado		
A.11.2.4 Mantenimiento de equipos	UPS defectuoso o sin mantenimiento	Plan de mantenimiento de equipos de cómputo. Contrato con el proveedor para el mantenimiento del UPS.	Director de Tecnologías de la Información y Comunicación	-	Implementado		
A.12.1.1 Procedimientos de operación documentados	Modificación no autorizada de información	Documentar los procedimientos del área de Tecnología, incluidos los procedimientos de gestión de la seguridad física y lógica.	Director de Tecnologías de la Información y Comunicación	-	5 meses	18-sep-2021	18-ene-2022
A.12.2.1 Controles contra códigos maliciosos	Código malicioso Modificación no autorizada de información. Virus contra computadoras	Adquisición y configuración de antivirus corporativo para todos los equipos de la red institucional. Revisión y actualización de las reglas del firewall existente.	Director de Tecnologías de la Información y Comunicación		Implementado		

A.12.5.1 Instalación de software en sistemas operativos	Código malicioso	Configurar mediante reglas del Directorio Activo existente, restricciones para instalación de software no autorizado.	Director de Tecnologías de la Información y Comunicación	-	Implementado		
A.12.7 Controles de auditorías de sistemas de información	Código malicioso Fraude	Ejecución de auditorías de sistemas, al menos una vez al año.	Director de Tecnologías de la Información y Comunicación	4.000,00	3 meses	18-ene-2022	18-mar-2022
A.14.2.1 Política de desarrollo de software	Código malicioso	Elaborar una política que incluya las directrices para el desarrollo de sistemas en la institución.	Director de Tecnologías de la Información y Comunicación	-	3 meses	18-sep-2021	18-nov-2021
A.14.2.5 Principios de construcción de los sistemas seguros	Código malicioso Fallas de Hardware en los equipos	Establecer, documentar, y mantener principios para la construcción de sistemas seguros y aplicarlos a cualquier actividad de implementación de sistemas.	Director de Tecnologías de la Información y Comunicación	-	3 meses	18-sep-2021	18-nov-2021
A.14.2.6 Ambiente de desarrollo seguro	Código malicioso	Mantener segregados los ambientes de pruebas y producción con los debidos controles de acceso.	Director de Tecnologías de la Información y Comunicación	-	3 meses	18-sep-2021	18-nov-2021

A.18.2.1 Revisión independiente de la seguridad de la información	Código malicioso Fraude Modificación no autorizada de información	Contratar un análisis de ethical hacking al menos una vez al año.	Director de Tecnologías de la Información y Comunicación	2.000,00	3 meses	18-dic-2021	18-feb-2022

ANEXO 7: CAPTURAS DE LA APLICACIÓN WEB DEL SISTEMA DE CITAS MÉDICAS


SISTEMA DE CITAS MEDICAS CLISAMARSA S.A.
Search
CLÍNICA SANTA MARTHA S.A
CLISAMARSA
LA LIBERTAD
Inicio
Citas
Pacientes
Medicos
Categorias
Reporte de Citas
Usuarios
Modificar Cita
Asunto
CITA MEDICA
Paciente
44 - MORALES FIGUEROA JORGE FRACISCO
Medico
1 - Dr. Felix Alejandro
Fecha/Hora
10/10/1976
16:30
Nota
Nota
Enfermedad
Enfermedad
Sintomas
Sintomas
Medicamentos
Medicamentos


SISTEMA DE CITAS MEDICAS CLISAMARSA S.A.
Search
CLÍNICA SANTA MARTHA S.A
CLISAMARSA
LA LIBERTAD
Inicio
Citas
Pacientes
Medicos
Categorias
Reporte de Citas
Usuarios
Historial de Citas del Medico
Medico: Dra. Nancy Morocho
Asunto
Paciente
Medico
Fecha
Dolor de Pecho
MARIANO MELESIO CACAO TOMALA
Dra. Nancy CACAO TOMALA
2020-10-22 18:00
Control
MARINA CECILIA TOMALA CATUTO
Dra. Nancy TOMALA CATUTO
2020-10-23 11:30
CONSULTA
FIDEL ERASMO MUÑOZ TOMALA
Dra. Nancy MUÑOZ TOMALA
2020-10-27 10:00
Control
SAYRA MIREYA SORIANO VILLON
Dra. Nancy SORIANO VILLON
2020-11-05 10:10
CONSULTA MEDICA
ISAIAS GABRIEL MUÑOZ TIGRERO
Dra. Nancy MUÑOZ TIGRERO
2020-11-08 10:30
Consulta
GLORIA MARIA TUMBACO DEL PEZO
Dra. Nancy TUMBACO DEL PEZO
2020-11-09 08:30
CONSULTA
PATRICIO REINALDO REYES FIGUEROA
Dra. Nancy REYES FIGUEROA
2020-11-10 09:00
CONSULTA
ADELAYDA MARILIN PINCAY QUIMIS
Dra. Nancy PINCAY QUIMIS
2020-11-10 10:57
Consulta
CRUZ ISABEL TOALA CEDEÑO
Dra. Nancy TOALA CEDEÑO
2020-11-26 16:30

ANEXO 8: SOLICITUD DE ENVIO Y ACEPTACIÓN PARA ACCEDER A LA INFORMACIÓN DE LA CLÍNICA

Facultad de
Sistemas y Telecomunicaciones
Tecnologías de la Información

UPSE

Oficio No. UPSE–CTI–382–2020–OF

La Libertad, 18 de diciembre del 2020

Asunto: Solicitud de Permiso Implementación Propuesta Tecnológica

Señora,
Dr. Nancy Del Rosario Morocho De La O
GERENTE PROPIETARIO
CLÍNICA SANTA MARTHA
La Libertad

De mi consideración:

Reciba un cordial saludo de la Carrera de Tecnologías de la Información de la Facultad de Sistemas y Telecomunicaciones de la Universidad Estatal Península de Santa Elena.

La Carrera de Tecnologías de la Información, con el objetivo de acrecentar los conocimientos teóricos y prácticos de los estudiantes e involucrar a los mismos en el desempeño particular de una empresa en las áreas de manejo sistemático de la información.

Conocedores de su apoyo al desarrollo en el campo educativo, ponemos a su consideración conceda la oportunidad al Sr. **CATUTO PILAY RICHARD MANUEL** con **C.I. 2400143570,** estudiante egresado de la carrera, de realizar las actividades inherentes a su propuesta tecnológica.

Agradeciendo de antemano por la deferente atención a lo solicitado, me suscribo de usted, reiterando mis sentimientos de alta consideración y estima.

Particular que comunico a usted para los fines pertinentes.

Atentamente,

CLINICA SANTA MARTHA
Dra. Nancy Morocho De La O
MEDICO CIRUJANO
CODIGO 1005266522

Ing. Samuel Bustos Gaibor
DIRECTOR DE LA CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN
Adjuntos
SB/Rg