UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN
SEGURIDAD DE LA INFORMACIÓN

RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:
ARTÍCULOS PROFESIONALES DE ALTO NIVEL

TEMA:
ANÁLISIS DE LAS VULNERABILIDADES DEL SISTEMA DE INFORMACIÓN ACADÉMICA: CASO DE ESTUDIO INSTITUTO SUPERIOR TECNOLÓGICO DEL AZUAY

AUTORES:
JOSÉ FABIÁN CHUQUI QUILLE
DANIEL ALEJANDRO ORELLANA GONZÁLEZ

DIRECTOR:
GALO ENRIQUE VALVERDE LANDÍVAR

CUENCA– ECUADOR
2023

Autores:

José Fabián Chuqui Quille
Ingeniero en Sistemas.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
jchuqui@est.ups.edu.ec

Daniel Alejandro Orellana González
Ingeniero Electrónico.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
dorellanag2@est.ups.edu.ec

Dirigido por:

Galo Enrique Valverde Landívar
Ingeniero en Computación.
Magister en Dirección Estratégica e Innovación de Tecnología.
gvalverde@ups.edu.ec

DEDICATORIA

Este trabajo está dedicado a todos quienes han colaborado durante el proceso de este, a mi esposa, mi hijo, mi familia, quienes fueron mi motivación y estuvieron presentes en buenos y malos momentos. Gracias a todos aquellos que me alentaron hasta cumplir con el objetivo y llegar al feliz término este proceso de formación y aprendizaje, a todos muchas gracias.

Fabián C.

Este trabajo de titulación lo dedico a mi mamá y a mi papá por ser una guía incondicional en todo mi aprendizaje, por ser luz en mis días de sombra y ser paz en mis momentos de angustia. También quiero dedicar este escrito a Dios por brindarme salud para poder desarrollar toda la planificación de este proyecto, serenidad cuando terminaba un capítulo, alegría cuando un objetivo se cumplía y felicidad cuando todo estaba listo para finalizar y entregar. No me puedo olvidar de agradecerme y dedicarme este material a mí mismo porque supe afrontar mis miedos, mis dudas y dedicarme por completo a superarme y graduarme.

Daniel O.

AGRADECIMIENTO

Al finalizar este proceso de tesis, quiero aprovechar este espacio para agradecer a Dios por todas sus bendiciones, a mi esposa e hijo por su apoyo incondicional en cada parte de este proceso, por su tiempo y paciencia. A mi compañero Daniel Orellana por su liderazgo, a nuestro tutor Galo Valverde y director de maestría Miguel Arcos, por su participación activa durante este proceso de estudio, también quiero hacer extensivo mi agradecimiento a las autoridades del Instituto Superior Universitario Tecnológico del Azuay, y todos aquellos que estuvieron de manera directa e indirecta y apoyaron a la realización y culminación de esta tesis.

Fabián C.

En este camino de dedicación, perseverancia y esfuerzo, agradezco a mis padres por apoyarme en este proceso de titulación, simpre estuvieron junto a mi alentándole. Doy gracias a Dios por escuchar mis oraciones y darme fuerzas cada día para completar un párrafo más de este manuscrito y a toda mi familia que son el pilar fundamental de mi vida, de mis metas y de mis objetivos.

Daniel O.

Tabla de Contenido

Índice de Figuras

Índice de Tablas

Análisis de las vulnerabilidades del sistema de información académica: Caso de estudio Instituto Superior Tecnológico del Azuay

Autor(es):

José Fabián Chuqui Quille

Resumen

El Instituto Superior al ser una institución de educación superior dispone de sistemas informáticos para la automatización de los procesos de enseñanza aprendizaje que facilitan la gestión de datos y la administración de la información.

La herramienta de software que sirve para el registro de notas, elaboración de sílabos, registro de datos personales de estudiantes y demás información académica se denomina Fénix y carece de controles adecuados de seguridad informática. En la encuesta realizada al personal académico no existe una cultura de protección de datos y seguridad de la información dentro del Instituto. Se dispone de un documento de Políticas de Seguridad, pero no se han podido implementar tales directrices, es por eso que es necesario un análisis de vulnerabilidades de seguridad y la integración de controles adecuados de protección.

La presente investigación tiene como objetivo el análisis las vulnerabilidades del sistema académico Fénix del Instituto Superior, a través de pruebas de hackeo ético y el uso de herramientas especializadas encargadas de presentar hallazgos de inseguridad informática mediante un diagnóstico exhaustivo y automático tomando como referencia el Estándar de Ejecución de Pruebas de Penetración (PTES). Para el análisis, se realiza una revisión bibliográfica del estado del arte relacionado a los métodos de análisis de vulnerabilidades más recientes implementados en instituciones de educación superior.

Al final de la presente investigación se propone un marco de políticas y recomendaciones de ciberseguridad para robustecer el sistema académico Fénix. Esta normativa incluye aspectos como: políticas de relación laboral, políticas de gestión de activos, políticas para la clasificación y etiquetado de información, políticas para la protección antimalware, políticas sobre el uso de internet, correos electrónicos y mensajería, políticas de gestión de riesgos, políticas en cuanto a la concientización de los usuarios, políticas de controles de seguridad, cifrado, registro de eventos, autenticación y gestión de contraseñas.

Palabras clave:
Sistema académico, pruebas de penetración, PTES, hackeo ético e ISO 27002.

ABSTRACT

The Instituto Superior, being a higher education institution, has computer systems for the automation of teaching-learning processes that facilitate data management and information administration.

The software tool that is used to register grades, prepare syllabi, record student personal data and other academic information is called Fénix and lacks adequate computer security controls. According to the survey carried out on academic staff, there is no culture of data protection and information security within the Institute. There is a Security Policies document, but it has not been possible to implement such guidelines, which is why an analysis of security vulnerabilities and the integration of adequate protection controls are necessary.

The purpose of this research is to analyze the vulnerabilities of the Fénix academic system of the Instituto Superior, through ethical hacking tests and the use of specialized tools in charge of presenting findings of computer insecurity through an exhaustive and automatic diagnosis taking as a reference the Penetration Test Execution Standard (PTES). For the analysis, a bibliographic review of the state of the art related to the most recent vulnerability analysis methods implemented in higher education institutions is carried out.

At the end of this research, a framework of cybersecurity policies and recommendations is proposed to strengthen the Fénix academic system. This regulation includes aspects such as: employment relationship policies, asset management policies, information classification and labeling policies, anti-malware protection policies, policies on the use of the Internet, emails and messaging, risk management policies, user awareness policies, security control policies, encryption, event logging, authentication, and password management.

Keywords:
Sistema académico, pruebas de penetración, PTES, hackeo ético e ISO 27002.

1 Introducción

El Instituto Superior, acoge actualmente alrededor de 1000 estudiantes y 80 docentes en las 19 carreras que oferta. Para llevar a cabo toda la gestión de los procesos de enseñanza aprendizaje el Instituto cuenta con equipos tecnológicos y sistemas de información que facilitan y automatizan varios procesos administrativos y académicos.

La seguridad de la información en equipos tecnológicos y sistemas de información tiene muy poca relevancia en la institución. Si bien se dispone de un documento aprobado que detalla las Políticas de la Seguridad, estas no se han implementado y no se ha levantado ningún control de ciberseguridad para garantizar la disponibilidad, confidencialidad e integridad de la información.

El poco interés en salvaguardar la seguridad de equipos tecnológicos y sistemas de información del Instituto del Azuay es preocupante y en necesario tomar acciones preventivas y correctivas ante amenazas de ciberseguridad. En este sentido y para marcar el comienzo de la implementación de seguridad de la información en el Instituto, se desarrolla como trabajo de titulación el análisis de las vulnerabilidades en el Sistema Académico Fénix del Instituto Superior. En este proceso, se contemplan, además, pruebas de hacking ético y la revisión documental de las políticas de seguridad propuestas.

El desarrollo del análisis de vulnerabilidades se inicia con un estudio bibliográfico de artículos internacionales, nacionales y locales de los últimos 5 años para poder desarrollar el levantamiento del estado del arte. En este apartado se estima la lectura de 20 manuscritos relacionados al análisis de vulnerabilidades en instituciones de educación superior. El estado del arte aportará significativamente al desarrollo efectivo de las pruebas para el hallazgo de vulnerabilidades, hackeo ético, y pruebas de penetración donde se podrá identificar la metodología más adecuada.

Como siguiente paso se planifica la ejecución de pruebas de seguridad sobre el sistema académico Fénix en donde se hace uso de herramientas de seguridad para el análisis de vulnerabilidades en el código fuente del aplicativo Fénix, hallazgos de inseguridades en el propio sistema y debilidades de ciberseguridad en los usuarios del sistema académico. Cabe señar que luego del análisis de vulnerabilidades se pretende desarrollar la explotación de las principales vulnerabilidades para verificar efectivamente la inseguridad latente.

Para finalizar el presente trabajo y luego del análisis y explotación de las vulnerabilidades encontradas, se pretende establecer un marco de políticas y recomendaciones de seguridad de la información para salvaguardar efectivamente al sistema académico Fénix de posibles eventos o incidentes de seguridad. En este proceso se planifica exponer las políticas para proteger al aplicativo en todos sus frentes mediante posibles recomendaciones que guarden relación con los hallazgos de inseguridad identificados.

1.1 Antecedentes

El Instituto Superior, es una casa de estudios de nivel superior que acoge actualmente alrededor de 1000 estudiantes y 80 docentes en las 19 carreras que ofrece. La seguridad de la información personal y académica de docentes y alumnos tiene muy poca

relevancia, y no se ha realizado ninguna gestión para garantizar la disponibilidad, confidencialidad e integridad de dicha información, misma que es considera sensible.

La Institución en su red interna de datos, gestiona alrededor de 128 computadores de los laboratorios más 80 computadores y 80 celulares de los docentes, todos estos conectados a la red LAN. Estos equipos cuentan con el servicio de internet, la mayoría tienen instalados sistemas operativos y programas piratas y trabajan con diferentes programas para el proceso de enseñanza/aprendizaje, siendo el sistema de información académico el más crítico por contener datos académicos sensibles.

Al no contar con un nivel de seguridad adecuado, la información contenida en los sistemas informáticos del Instituto se ve comprometida a cualquier tipo de delito o ataque informático; el problema que el ISTA afronta con respecto a la seguridad de la información en el ámbito tecnológico se puede sustentar en los siguientes puntos:

- No se ha realizado hasta la fecha un análisis de vulnerabilidades en el Instituto.
- Se dispone de una política de protección de la información, pero no han sido aplicada ni evaluada.
- No existe concientización ni formación en seguridad de la información.
- Otros inconvenientes que puede presentarse a corto plazo de no integrarse las buenas prácticas en seguridad son:
- Ataques de robo y manipulación de la información personal y académica.
- Ataques de softwares maliciosos.

En estos últimos cuatro años (2019 - 2022) se detectaron 3 ataques, dos de fuerza bruta y uno de malware.

El primer ataque de Fuerza Bruta se suscitó en febrero del 2019, el equipo atacado fue el router principal, el usuario atacado fue el usuario administrador del router, el evento empezó desde las 10:00 horas del día 5 hasta las 11:26 horas del día 7 de febrero, con un intervalo de 25 segundos. Esta alerta fue detectada por el administrador del router quien agregó 2 reglas en el firewall para bloquear las IPs desde donde provenía el ataque, se tomó la decisión de cambiar el nombre de los usuarios y contraseñas.

El ataque de Malware se detectó el día 18 de septiembre del año 2020, fue detectado por los antivirus de algunos docentes que reportaron a la Unidad de TICs; no se pudo detectar la máquina que estaba infectando a los equipos de la red LAN y los antivirus no detectaban la IP pero si el puerto, por lo que se bloqueó el puerto 2085 en el firewall.

El segundo evento de ataque de Fuerza Bruta se dio el 7 de mayo del año 2022, el equipo atacado fue el router principal. El afectado fue el usuario administrador del router y el ataque empezó desde las 10:00 horas hasta las 10:26 horas, con un intervalo de 10 segundos, esta alerta fue detectada por el administrador mediante el reporte de eventos del router, para solventar el problema se agregó una regla en firewall para bloquear las IPs de donde procedía el ataque y se deshabilitó el puerto Telnet.

Así mismo, se pueden evidenciar dentro del Instituto el incorrecto manejo y gestión de los servicios y servidores; en el año 2021 se realizó una actualización del servidor principal del instituto, este proceso se realizó con un respaldo de 8 meses anteriores y, por la mala gestión y coordinación técnica, se perdió información de 5 meses, debido a un error en las fechas de los backups.

La seguridad de la información debe estar presente en todos los sectores especialmente en los institutos, universidades, y casas de estudio con carácter público y privado. Todas las organizaciones y empresas pueden en algún momento ser víctimas de alguna estafa o ataque directo. Hasta el primer trimestre del 2022 en el Ecuador existen 97 institutos técnicos y tecnológicos acreditados y 55 universidades entre públicas y privadas [1], por lo que salvaguardar estas vulnerabilidades de seguridad no es un tema menor.

La encuesta realizada al personal académico refleja que el 71% no ha recibido algún tipo de capacitación o concienciación de seguridad de la información por parte del Instituto. Así mismo, el 80% los docentes encuestados afirman que no existe una cultura de protección de datos y seguridad de la información.

Los ataques de seguridad de la información se presentan en formas distintas, por lo que la mayoría de instituciones públicas y privadas del Ecuador se ven comprometidas al no tener mecanismos de detección y defensa [2] [3] [4]. Además, existe poca capacitación y concienciación acerca de la seguridad de la información en las instituciones académicas del país dando lugar a una deficiente cultura de protección de datos.

1.2 Determinación del problema

En los últimos cuatro años entre el 2019 y el 2022 en la infraestructura de tecnología y comunicación del Instituto Superior se han detectaron 3 ataques, dos de fuerza bruta y uno de malware, sin embargo, no se han establecido y aplicado políticas de seguridad para salvaguardar la información de los datos académicos y personales de estudiantes y docentes de esta institución de educación superior.

El primer ataque se suscitó en febrero de 2019 donde el equipo víctima fue el router principal. Esta explotación brindo acceso al router con usuario administrador. El equipo de Tecnología y Comunicación del Instituto logró subsanar este incidente con la aplicación de una regla de firewall. El segundo ataque tipo Malware se detectó el día 18 de septiembre del año 2020 por la acción de un antivirus. El software malicioso ingresó por el puerto 2085 y se logró la mitigación de este incidente cerrando el puerto. El tercer evento de ataque de Fuerza Bruta tuvo lugar el 7 de mayo del año 2022, el equipo atacado fue el router principal nuevamente. Se subsano este incidente de seguridad agregando reglas en firewall para bloquear las direcciones IPs de donde procedía el ataque.

La seguridad de la información del Instituto Superior no esta ni siquiera en una fase inicial debido a la falta de interés de la Institución en salvaguardar su información. Los

acontecimientos de inseguridad que ha experimentado en Instituto no han sido razones suficientes para tomar en serio la protección de los activos de información de la Institución por lo que la protección que actualmente tienen la infraestructura de tecnología y comunicación del Instituto es muy pobre.

Para evidenciar de mejor manera la inseguridad de la información se realizó una encuesta al personal académico del Instituto para conocer su percepción. Los resultados de esta encuesta indican que el 71% de los encuestados no ha recibido algún tipo de capacitación o concienciación de seguridad de la información por parte del Instituto. Así mismo, el 80% los docentes encuestados afirman que no existe una cultura de protección de datos y seguridad de la información dentro de las instalaciones de la entidad académica.

Con todos estos estos antecedentes de inseguridad informática, el presente trabajo de titulación pretende marcar el inicio de una correcta planificación e implementación de un sistema de seguridad de la información dentro del Instituto del Azuay en donde se disponga de una protección efectiva de la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información institucional.

1.3 Justificación

Las vulnerabilidades de la seguridad de la información, no sólo están presentes en el Ecuador sino a nivel mundial en donde muchas empresas internacionales buscan proteger y salvaguardar la información sensible [5]. Evitar el robo y el mal uso de esta información es cada vez más primordial en estos tiempos, donde los ataques y ciber amenazas se dan con mayor frecuencia en busca de obtener beneficios. En junio de 2022, según el mapa de ataques en tiempo real del portal web de Kaspersky [6], Rusia se encuentra encabezando la lista de los países con mayor número de ataques y el Ecuador se ubica en el puesto 39. Según el mismo portal, los ataques de Ransomware en Ecuador subieron de 78 a 1167 por poner un ejemplo.

Los ciberataques a infraestructuras públicas o privadas desencadenan intranquilidad [7] [8] [9], debido ha que la penetración de estos ataques informáticos proporciona perdidas o buscan desprestigiar a los gobiernos y compañías [10] [11] [12].

Las instituciones académicas forman parte de los establecimientos afectados por los ciberdelitos que se están suscitando actualmente [13], los atacantes informáticos buscan sustraer pruebas y datos científicos de investigaciones que no han sido publicadas. Siendo las instituciones educativas un blanco para los atacantes, que no solo buscan robar información sino también buscan remuneración económica a cambio de los datos secuestrados. Sólo en USA, en 2020, incluidos los costos de tiempo de inactividad, reparaciones y oportunidades perdidas, el ataque promedio de Ransomware fue de 1.681 escuelas, colegios y universidades, costó a las instituciones educativas $ 2.73 millones. Fuera de USA, el 44% de las instituciones educativas fueron blanco de ataques [14].

El Instituto Superior, es una institución de educación superior en donde la falta de seguridad de la información académica, y se puede desencadenar una serie de problemas que atenten a la confidencialidad, autenticidad, disponibilidad y privacidad de los datos de toda la comunidad académica. La Ley Orgánica de Protección de Datos Personales vigente en Ecuador desde el 26 de mayo de 2021, en su artículo 24 indica que:

> Art. 24.- Ejercicio de derechos.- El Estado, entidades educativas, organizaciones de la sociedad civil, proveedores de servicios de la sociedad de la información y el conocimiento, y otros entes relacionados, dentro del ámbito de sus relaciones, están obligados a proveer información y capacitación relacionadas con el uso y tratamiento responsable, adecuado y seguro de datos personales de niñas, niños y adolescentes, tanto a sus titulares como a sus representantes legales, de conformidad con la normativa técnica emitida por la Autoridad de Protección de Datos Personales [15].

Según el Acuerdo Ministerial 006-2021de las Política de Ciberseguridad aprobada el 17 de mayo de 2021 se menciona que:

> La política establece directrices que buscan afianzar un ciberespacio seguro para contribuir al desarrollo social, económico y humano del país, así como a la creación de una confianza digital que favorece el intercambio de información y, en consecuencia, de bienes y servicios en línea [15].

Algunos trabajos relacionados sobre análisis de vulnerabilidades en instituciones educativas del Ecuador, destacan detalles de la metodología para este proceso. En estos trabajos se propone un escaneo de vulnerabilidades de la red LAN con NESSUS, en otro artículo se realiza la aplicación de hacking ético mediante un test de intrusión y ataques "Man in the Middle". En otro estudio se detalla una auditoría de seguridad informática que propone desarrollar como primera etapa un reconocimiento a la infraestructura física y tecnológica, en la segunda etapa la clasificación de los activos por criticidad, definiendo los planes a desarrollarse y obtener datos donde se identifique el estado de seguridad de hardware y software, por último en la tercera etapa se especifica la realización pruebas, basadas en herramientas de escaneo y análisis para poder detectar posibles vulnerabilidades. En un estudio asi mismo, se realiza la ejecución del análisis utilizando la guía que proporciona Open Web Application Security Project (OWASP) para pruebas de seguridad en sistemas informáticos.

El trabajo de titulación propuesto, busca identificar las inseguridades que tiene el sistema académico Fénix, el cual es utilizada principalmente por los docentes del instituto para el registro de datos académicos, también este sistema provee información a otros sistemas como el sistema de evaluación docente, sistema de talento humano y sistema de activos fijos, la información comprometida es la siguiente:

- Información personal de la comunidad.
- Especificaciones de periodos académicos.
- Detalles de carreras, asignaturas y horarios.

- Datos de matrículas.
- Estudiantes matriculados, retirados y desertores.
- Documentos académicos como sílabos, planes de clase, avances de sílabo.
- Registros de notas parciales y finales.
- Asistencia de los estudiantes.
- Base de datos de la biblioteca.
- Comprobantes de pago.
- Reportes.
- Entre otros.

Todos estos datos son críticos y se encuentran asociados a los 1000 estudiantes y 80 docentes con los que cuenta esta casa de estudios y son cruciales para toda la planificación, gestión y administración del Instituto. Es imprescindible realizar un análisis de las vulnerabilidades de este sistema académico. No se tiene conocimiento de cómo se encuentra esta plataforma en temas de seguridad de la información, así mismo se busca realizar este estudio para obtener resultados e indicadores que reflejen el estado actual en el que se encuentra este sistema y su información dentro de la institución.

Otra de las razones por las que se desea desarrollar este análisis de vulnerabilidades es para proponer un marco de políticas y recomendaciones que ayudarían al mejoramiento de la seguridad del sistema académico del Instituto Superior.

1.4 Objetivos

Objetivo General:

Analizar las vulnerabilidades de la información alojada en el Sistema Académico del Instituto Superior Tecnológico del Azuay, a través de pruebas de hacking ético a los servidores del sistema académico y de la revisión documental de las políticas de seguridad.

Objetivos Específicos:

- Realizar una revisión del estado del arte relacionado al tema del trabajo de titulación.
- Ejecutar una planificación de hackeo ético que contemple un análisis de vulnerabilidades al sistema académico del Instituto.
- Proponer un marco de políticas y recomendaciones para robustecer el sistema de información académica.

2 Marco teórico referencia

Este proyecto se desarrolló con el objetivo, de realizar el análisis de la seguridad de la información dentro del Instituto Superior, y por medio relevamiento de datos e información de una amplia variedad de fuentes utilizadas en la toma de decisiones sobre el las vulnerabilidades encontradas del sistema académico, como respuesta a los incidentes de seguridad de la información en la institución. En este apartado se desarrolla una revisión exhaustiva de investigaciones, tesis y artículos científicos que hacen referencia al análisis de vulnerabilidades de seguridad de la información en Instituciones educativas, con el fin de informar los resultados encontrados sobre esta temática, para alcanzar esta meta se revisará la literatura internacional, nacional y local de los últimos 5 años para disponer de casos de estudio recientes.

Es importante recalcar que los documentos a tratar fueron consultados desde fuentes oficiales y corresponden a algunos análisis de seguridad de la información realizados a Instituciones de Educación Superior y se les agrupo de acuerdo a los criterios de tipo y metodología del análisis de vulnerabilidad del sistema académico: Análisis Integrales de Sistemas Académicos, Análisis de vulnerabilidades web, e Investigaciones de auditoría con Análisis de Riesgos e implementación de Sistemas de Gestión de la Seguridad

2.1 Artículos sobre el análisis de vulnerabilidades en sistemas académicos

En noviembre de 2017 [14], fue implementada una investigación que utilizaba una aplicación de inteligencia de negocios para el análisis de vulnerabilidades e incrementar el nivel de seguridad de un equipo académico de respuesta ante incidentes informáticos denominado con sus siglas en ingles CSIRT (Computer Security Incident Response Team). Este estudio fue desarrollado por un grupo de investigadores académicos que agrupa varias universidades miembros del CSIRT en Ecuador. La aplicación de herramientas como Passive Vulnerability Scanner y Snort, ayudaron en la extracción, transformación y carga de logs de los incidentes registrados, y con la herramienta Pentaho BI se presentó algunas vulnerabilidades encontradas por el equipo CSIRT.

En octubre de 2018 fue presentada por la revista Electrónica de Computación e Informática de la Universidad de Guadalajara una investigación [15], en la que se consideraron estrategias de gestión de seguridad informática con base en la metodología Open Source Security Testing Methodology Manual (OSSTMM) para la Intranet de una Institución de Educación Superior de la ciudad de Guayaquil en Ecuador. Se utilizaron las herramientas de hacking ético y se encontraron las vulnerabilidades, tanto como los controles adecuados de políticas de seguridad informática y aplicación de las mismas; no disponía de una protección adecuada apoyada con IPS/IDS, o antivirus

bajo licencia para la detección de posibles amenazas, además que, se identificaron 146 puntos activos de acceso y visibilidad.

En mayo del 2019 la revista Ibérica de Sistemas y Tecnologías de Información muestra una investigación realizada en las universidades: Técnica de Manabí (UTM), Laica Eloy Alfaro de Manabí (ULEAM), Escuela Superior Politécnica, Agropecuaria de Manabí Manuel Félix López (ESPAM MFL) y Estatal del Sur de Manabí (UNESUM) [16] donde publicaron un artículo que busca medidas estratégicas relevantes en cuanto al control correctivo y, de ser el caso, preventivo en estas entidades, debido a que son instituciones que manejan volúmenes de información importantes y que deben ser protegidas de los atacantes cibernéticos. Las herramientas y métodos utilizados para buscar vulnerabilidades dentro de estas entidades educativas fueron: cuestionarios basados en la norma ISO/IEC 27032, metodología AMFE, Shodan, Nessus, y Acunetix, además se encontraron varias vulnerabilidades dentro de los sistemas administrativos y educativos como también en los servidores.

En enero de 2020 en la Universidad Distrital Francisco José de Caldas fue publicado un artículo sobre el análisis de ataques informáticos a través de Honeypots para mejorar la seguridad de esta institución [17]. Este estudio se llevó a cabo con la metodología PDCA (Planificar - Hacer - Verificar - Actuar) y se desarrolló un script que se inserta en el servidor IDS que hace el papel de Honeypots para detectar posibles intrusiones. Las herramientas utilizadas son el Cowrie y HoneyPy, Honeypots, conexiones SSH y telnet; los resultados indican que algunas direcciones públicas de sitios como Cymon, DeShield, OTX, Twitter, Google, habían intentado ingresar al sistema.

La Escuela Politécnica Nacional en el año 2020 [18] incluye una investigación sobre la estrategia para la evaluación de vulnerabilidades del sistema de notas de instituciones educativas utilizando técnicas de hacking ético mediante el análisis de caso del Instituto Tecnológico Quito. Se utilizaron herramientas como NetCraft, DomainTools, Nmap, OWASP ZAP, ataques de ClickJacking (secuestro de clicks), WAPPALYZER, Nikto, Firefox, SQLmap ; los resultados de este estudio de seguridad informática muestran la obtención de IP pública del sitio, se descubre el nombre de dominio y proveedor, el tipo de servidor y la IP, puertos abiertos, descubrimiento del framework (Microsoft ASP.NET), sistema operativo del servidor y el servidor web (IIS), posibilidad de ejecutar sentencias para XSS, sistema de notas vulnerable a inyección SQL, notas vulnerables a clickjacking.

En noviembre de 2020 la Revista de Ciencia y Tecnología Ingenius [19] publica un artículo sobre análisis de vulnerabilidades con Sqlmap aplicada a entornos de Oracle APEX 5 mediante el manejo de herramientas FOSS de prueba, suite KALI, herramienta SQLMap. Las evidencias de las pruebas indicaron que no se permite acometer el software APEX con la técnica de inyección SQL. Por otra parte, la técnica de la captura de la cookie no dio resultado y en este caso Oracle APEX genera otra cookie a tiempo. Este estudio se llevó a cabo en las instalaciones de la Universidad del Azuay de la Ciudad de Cuenca.

En marzo del 2021 la Universidad Técnica de Moldova [20] presenta la investigación realizada de un análisis de amenazas y vulnerabilidades de seguridad cibernética, en la cual se identificaron amenazas en la educación superior a distancia en los equipos de

computación de la nube, sistemas de gestión de aprendizaje y aplicaciones de videoconferencia, tales como vulnerabilidades de tecnologías compartidas, secuestro de tráfico de cuentas o servicios, denegación de servicio, información maliciosa, comunicaciones inseguras, gestión de sesiones activas y no autorizadas, fuga de información y manejo inadecuado de errores, ejecución de archivos maliciosos, descifrado de videos y audios. Las soluciones de controles de seguridad que resultaron de este estudio son la actualización de sistemas y parches de seguridad, controles de acceso, políticas de seguridad, uso de protocolos de seguridad, encriptación, capacitación de estudiantes y docentes en temas de seguridad de la información.

La Institución Educativa de la Provincia de Santa Elena, Ecuador, en marzo de 2021 [21] finaliza un trabajo de grado que aplica la metodología de Hacking Ético mediante test de intrusión "pentesting", para la detección y análisis de vulnerabilidades en la red inalámbrica. En esta intervención se utilizaron herramientas de ciberseguridad Kali, Nmap, Vulnerabilidad de Exposición Común CVE, Mitre-CVE, CVE-ID, VirtualBox, Metasploit, Ettercap, WireShark entre otros. Los resultados obtenidos en este caso fueron ciertos puertos con vulnerabilidades, servicios FTP vulnerables, Telnet, Domain, Http, SSL, http-proxy, Msrpc, NetBios-ssn, Microsoft-ds, red vulnerable a ataques Sniffing y Man in the middle.

En octubre de 2021 la Universidad VWX de Indonesia [22] presenta una investigación donde se utilizaron pruebas estándares de penetración para realizar un análisis de la seguridad del sistema de información, e indagar en las vulnerabilidades de ciberseguridad del servidor que provee este servicio. En este caso se utilizan herramientas como PTES, Nmap, Nessus, Whois, Metasploit y WireShark, y se encontraron vulnerabilidades en algunos sitios, además de que se realiza la explotación de registros confidenciales, descubrimiento de contraseñas, infiltraciones de acceso al servidor y puertos abiertos.

En el 2021 se publicó un trabajo de grado desarrollado en la Universidad Politécnica Estatal del Carchi en Ecuador [23], donde se desarrollaron pruebas de penetración de seguridad informática al servidor web del laboratorio de ciberseguridad. El estudio encontró algunas vulnerabilidades como: el descubrimiento de claves de acceso, puertos abiertos, vulnerabilidades tipo GET y POST, acceso a los directorios, inyección XXS, vulnerable a ataque DoS, falta de integridad, confidencialidad y disponibilidad de los datos.

La Universidad Técnica de Babahoyo en noviembre de 2021 [24] finaliza un trabajo de investigación acerca del análisis de las vulnerabilidades de la red LAN del distrito de educación 12D02 Pueblo viejo-Urdaneta, en donde se obtiene con la ayuda de las herramientas de seguridad informática como Nmap, Nessus y Zenmap los siguientes resultados: puertos abiertos, mala ubicación de dispositivos, fallas en la instalación y configuración de redes.

En la tabla 01 se resume las primeras investigaciones referentes al análisis de vulnerabilidades de sistemas académicos

Tabla 1: Artículos sobre el análisis de vulnerabilidades en sistemas académicos

Lugar y fecha de publicación	Título del documento	Vulnerabilidades encontradas	Herramientas utilizadas	Metodología
Universidad Pedagógica y Tecnológica de Colombia / Noviembre 2017.	Application of business intelligence for analyzing vulnerabilities to increase the security level in an academic CSIRT.	Vulnerabilidades encontradas por CSIRT.	Herramientas de análisis de intrusos: Passive Vulnerability Scanner y Snort. Extracción, transformación y carga de logs de los incidentes registrados, herramienta Pentaho BI.	Investigación con un enfoque cualitativo para el análisis de vulnerabilidades. Fase 1: comparativa de dos herramientas de análisis de intrusos. Fase 2: Extracción, transformación y carga de logs de los incidentes registrados. Fase 3: construcción de una aplicación para análisis inteligente con logs obtenidos con el propósito de generar alertas tempranas como un factor estratégico.
Revista electrónica de Computación, Informática, Universidad de Guadalajara México. / octubre 2018.	Análisis de Estrategias de Gestión de Seguridad Informática con Base en la Metodología Open Source Security Testing Methodology Manual (OSSTMM) para la Intranet de una Institución de Educación Superior.	Control y aplicación inadecuada de políticas de seguridad informática, no se dispone de una protección adecuada apoyada con IPS/IDS. Antivirus bajo licencia para la detección de posibles amenazas. 146 puntos interactivos de acceso y visibilidad.	Utilizando como tipo de prueba el Hacking ético.	Metodología OSSTMM para aplicar una auditoría de seguridad informática e identificar vulnerabilidades de seguridad en la Institución de Educación Superior.
Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López/ mayo del 2019	Ciberseguridad y su aplicación en las Instituciones de Educación Superior	El total de vulnerabilidades obtenidas de los sistemas distribuidos analizados de la ESPAM MFL es de 1.499; para la ULEAM es de 1 571, para la UNESUM, 1 164 y para la UTM, de 2 772 vulnerabilidades	Cuestionarios basados en la norma ISO/IEC 27032, matriz AMFE, Shodan, Nessus, y Acunetix.	Metodología Análisis Modal de Fallos y Efectos (AMFE) se brindó soluciones de mitigación de riesgos.
Universidad Distrital Francisco José de Caldas. Bogotá – Colombia. / enero 2020.	Analysis of computer attacks through Honeypots in the District University Francisco José de Caldas.	Se observan las direcciones IP y sitios web que intentan acceder al sistema detectadas por los Honeypots. Entre los sitios están: Cymon, DeShield, OTX, Twitter, Google, entre otros.	Script en el servidor IDS, Cowrie y HoneyPy, Honeypots, conexiones SSH y telnet.	Se utiliza el ciclo PDCA (Planificar - Hacer - Verificar - Actuar). Implementación de Cowrie y HoneyPy en el servidor IDS.
Escuela Politécnica Nacional / 2020.	Estrategia para la evaluación de vulnerabilidades del sistema de notas de instituciones educativas utilizando técnicas de hacking ético. Caso de estudio: Instituto Tecnológico Quito.	Obtención de: IP pública del sitio, dominio, proveedor, nombre de dominio, tipo de servidor, IP, puertos abiertos, framework (Microsoft ASP.NET), sistema operativo del servidor, servidor web (IIS). Vulnerable a inyección SQL y clickjacking.	NetCraft, DomainTools, Nmap, OWASP ZAP, sistema de notas es propenso a recibir ataques de ClickJacking, WAPPALYZER, Nikto, Firefox, SQLmap.	Se realiza la ejecución del análisis utilizando la guía que proporciona OWASP para pruebas de seguridad en sistemas informáticos.

Universidad Politécnica Salesiana / noviembre 2020.	Análisis de vulnerabilidades con sqlmap aplicada a entornos APEX 5 / noviembre 2020.	No se permitió acometer el software con la técnica de inyección SQL. La técnica de la captura de la cookie no dio resultado y Oracle APEX generó otra cookie a tiempo.	Herramientas FOSS de prueba, suite KALI, herramienta SQLMap.	La primera prueba consistió en listar las bases de datos; en la segunda, se aumentó el grado de agresividad y cantidad de pruebas para obtener información de las bases de datos; y en el tercer ataque se pretendió usar un agente aleatorio evadiendo los proxys con el único propósito de capturar una cookie de sesión para simular una sesión válida de un usuario activo.
Technical University of Moldova - Moldovia / International Journal of Scientific & Technology Research/ Marzo 2021.	Análisis de amenazas de ciberseguridad en instituciones de educación superior como resultado de la educación a distancia.	Se identificaron amenazas en Cloud Computing, Learning Management Systems (LMSs) y Video conferencing applications (VCA) y las soluciones de seguridad para cada una de estas herramientas educativas.	Revisión bibliográfica.	Revisión de la literatura en sitios como IEEE Xplore, ScienceDirect, Kaspersky y SpringerLink entre el 2011 al 2020. Además de consultas de informes de seguridad.
Universidad Estatal Península de Santa Elena / marzo 2021.	Aplicación de hacking ético mediante test de intrusión “pentesting” para la detección y análisis de vulnerabilidades en la red inalámbrica de una institución educativa de la provincia de Santa Elena.	Ciertos puertos con vulnerabilidades, servicios vulnerables FTP, Telnet, Domain, Http, SSL, http-proxy y desconocidos, Msrpc, NetBios-ssn, Microsoft-ds, red vulnerable a ataques Sniffing y MITM.	Kali, NMAP, Vulnerabilidad de Exposición Común CVE, Mitre-CVE, CVE-ID, VirtualBox, Metasploit, Ettercap, WireShark, Adaptador inalámbrico WIFI.	Se realiza la aplicación de Hacking Ético mediante un Test de Intrusión “Pentesting” y ataques Man in the Middle (MITM). Se lleva a cabo taques mediante Exploit HTA Web Server y Windows 10. Ataques MITM ARP-Spoofing o ARP-Poisoning.
International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS) / October 2021.	Information System Security Analysis to Determine Server Security Vulnerability with Penetration Testing Execution Standard (PTES) Method at VWX University.	Ataques de rastreo entre sitios (CST), Exposición de datos confidenciales, adivinación de contraseñas, ataque DDoS y Actividades de rastreo que infligen acceso al sistema del servidor. Puertos abierto en IP xxx.xxx.92.2 : 21, 22, 80, 443, 5432.	Estándar de Ejecución de Pruebas de Penetración (PTES), Nmap, Nessus, Whois, Marco Metasploit, WireShark.	Las técnicas utilizadas son explotación, rastreo, adivinación de contraseñas, servicio de escaneo, Nmap.
Universidad Politécnica Estatal del Carchi / septiembre 2021.	Pruebas de penetración para la seguridad informática al servidor web del laboratorio de ciberseguridad en la Universidad Politécnica Estatal del Carchi.	Descubrimiento de claves de acceso, puertos abiertos, vulnerabilidades tipo GET y POST, acceso a los directorios, inyección XXS, falta de integridad, confidencialidad y disponibilidad de los datos, vulnerable a ataque DoS.	OWASP Zap, Nmap, Acunetix, Curl, y plataformas web como whois, web server tolos, entre otros.	Se basa en el análisis de vulnerabilidades en los servidores web de Apache sobre Centos 7.0 y Microsoft IIS sobre Windows Server 2016 a través de herramientas Pentest y apoyada en la metodología Open web Applications Security Project (OWASP).
Universidad Técnica de Babahoyo / noviembre 2021.	Análisis de las vulnerabilidades de la red LAN del Distrito de Educación 12d02	Puertos abiertos de algunas computadoras, switches mal ubicados, fallas en instalación y configuración de la red LAN.	Entrevistas, herramienta de análisis de riesgos Nessus, Nmap, Zenmap.	Escaneo de vulnerabilidades de la red LAN con Nessus. Descriptiva.

	Puebloviejo – Urdaneta.			

2.2 Artículos sobre análisis de vulnerabilidades web

En el 2018 dentro de la serie de conferencias IOP (Institute of Physics) [25] fue presentado un artículo en el cual se desarrolló un análisis de vulnerabilidades en tres sitios web de la Universitas Komputer de Indonesia para luego proceder a fortalecer la seguridad en las mismas. Las herramientas utilizadas en este caso son Zenmap, Nikto XSS, OWASP Dir Buster, ViSQL; entre las vulnerabilidades encontradas se tiene: puertos abiertos, Http trace activo, Cross Site Tracing, XSS Bugs, directory-list no encontrado, y SQL injection. La solución propuesta para mejorar la seguridad consiste en reparar los sitios web con http-Access y corregir el método de secuencias de comandos.

En febrero de 2018 se presentó un trabajo de grado en la Universidad Nacional Abierta y a Distancia –UNAD [26], en la cual se realizó un análisis y evaluación de la seguridad informática de la página web publicada en un hosting gratuito de la Institución Técnica de Firavitoba, en la ciudad de Sogamoso de Colombia, para la detección y remediación de vulnerabilidades y riesgos en la información. En este estudio se utilizaron las herramientas de Owasp, Skipfish, Sucuri, y se detectaron algunas vulnerabilidades de seguridad de la información en la página web susceptibles a ataques ClickJacking; la página incluye uno o más archivos de script de un dominio de terceros, sitio propenso a ataques Cross Site Scripting por no tener habilitada la protección XSS, y se podía copiar el contenido y código de la página con facilidad.

En febrero del 2019 en la Universidad Técnica de Machala [27], se publicó un estudio de los ataques a la página web de la institución, así como también un análisis de las vulnerabilidades y amenazas. La metodología utilizada se basa en entrevistas y revisión bibliográfica. Dentro de los principales problemas de seguridad que se identificaron son: falta de mantenimiento, inadecuada inspección y exploración del sitio, escasa evaluación de protocolos de seguridad web y falta de verificación de información pública.

En enero del 2020 se presentó el trabajo de investigación de la Universidad Laica Eloy Alfaro de Manabí Extensión El Carmen [28], en el cual se implementa la metodología OWASP para identificar vulnerabilidades en los sistema informáticos como también en las redes de esta unidad de educación. Los resultados identificaron varias inseguridades en puertos, firewall, backlog y contraseñas débiles.

En noviembre 2021 se presenta una investigación realizada en el Instituto Superior Tecnológico José Ochoa León de Ecuador [29], en la cual se implementó una metodología basada en la guía de pruebas de seguridad web de OWASP, lo cual permitió identificar y corregir vulnerabilidades dentro de las configuraciones, tanto en la aplicación web Moodle como en el servidor web Apache, mediante el uso de herramientas automatizadas como

OWASP ZAP, NESSUS, WireShark y Nmap, aplicando testeos, escaneos de puertos, servicios y flujo de datos.

En la tabla 2 se resume las investigaciones referentes al análisis de vulnerabilidades web académicas.

Tabla 2: Artículos sobre análisis de vulnerabilidades web

Lugar y fecha de publicación	Título del documento	Vulnerabilidades encontradas	Herramientas utilizadas	Metodología
Universitas Komputer Indonesia, Jl. Dipatiukur 102-116 Bandung, West Java, Indonesia, 2018.	Análisis e implementación de vulnerabilidades web.	Puertos abiertos, Http trace activo, Cross Site Tracing, XSS Bugs, directory-list no encontrado, y SQL injection.	Zenmap, Nikto XSS, Owasp Dir Buster, ViSQL.	Se realiza el análisis de vulnerabilidades y luego se repara el sitio web con http-Access y se corrige el método de secuencias de comandos.
Universidad Nacional Abierta y a Distancia –UNAD Escuela de Ciencias Básicas, Tecnología e Ingeniería Especialización en Seguridad Informática Sogamoso Boyacá / Febrero 2018.	Análisis y evaluación de la seguridad informática para la página web publicada en hosting gratuito de la Institución Técnica de Firavitoba, para la detección y remediación de vulnerabilidades y riesgos en la información.	Página web susceptible a ataques "ClickJacking" , La página incluye uno o más archivos de script de un dominio de terceros, sitio propenso a ataques Cross Site Scripting por no tener habilitada el Protección XSS, se puede copiar el contenido y código de la página con facilidad.	Owasp, Owasp Zap, Skipfish, Sucuri, ISO 27000.	La metodología para la detección de vulnerabilidades y riesgos en la página web es el Top 10 de OWASP con su herramienta de trabajo OWAPS ZAP (Zed attack proxy), la cual será instalada y ejecutada.
Universidad de Machala, Carrera de Contabilidad y Auditoría. / febrero de 2019.	Análisis de vulnerabilidades, amenazas y ataques a la página web de la Universidad Técnica de Machala.	Falta de mantenimiento, inadecuada inspección y exploración, escasa evaluación de protocolos de seguridad, falta de verificación de información pública.	Entrevistas, verificación en campo, constatación y pruebas de conexión.	Investigación documental en donde se utilizan entrevistas a la persona encargada del sitio web institucional y a la dirección de TIC.
Universidad Laica Eloy Alfaro de Manabí / enero del 2020	Análisis de seguridad mediante metodología OWASP a redes inalámbricas en “Universidad Laica Eloy Alfaro de Manabí Extensión El Carmen”	Vulnerabilidades en puertos 1111, 9876 , Causa problemas en el Firewall Conexiones no cerradas de destino remoto, Detección de Backlog, Contraseñas débiles	OWASP, SQL Injection, NESSUS, Wireshark	Metodología OWASP es la encargada de analizar las posibles vulnerabilidades
Instituto Superior Tecnológico José Ochoa León, Ecuador/ enero 2022	Análisis de factores de seguridad informática mediante la metodología OWASP v4.2: Caso de estudio ISTJOL	vulnerabilidades dentro de las configuraciones, tanto en la aplicación web Moodle como en el servidor web Apache	OWASP ZAP, NESSUS, Wireshark y Nmap	metodología basada en la guía de pruebas de seguridad web de OWASP

2.3 Artículos sobre investigaciones de auditoría, análisis de riesgos e implementación de Sistemas de Gestión de la Seguridad

En la Institución Educativa Departamental Luis Carlos Galán - Municipio de Yacopí Cundinamarca en Colombia, en octubre de 2017 [30] se lleva a cabo una auditoria de seguridad informática. Las vulnerabilidades encontradas fueron: puertos abiertos, fallos a nivel de sistemas operativos, aplicativos o servicios, vulnerabilidades tipo ransomware, alto riesgo de amenazas y vulneración en servidores web, denegaciones de un servicio, malas prácticas para la asignación de passwords. Los utilitarios de seguridad que se utilizaron fueron: Nmap, ping, Zenmap, Nessus, Nikto, y John The Ripper.

En noviembre del 2018 se presenta un trabajo de grado realizado en la Universidad Estatal del Sur de Manabí en Ecuador [31], en la cual se lleva a cabo el diseño de un modelo de gestión de seguridad de la información para el sistema académico de esta institución educativa. En esta investigación se describen principalmente los riesgos del sistema académico y los detalles de la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI).

Un artículo realizado en la Universidad Nacional de Piura – Perú, en julio del 2019 [32], desarrolló el diseño de un sistema de gestión de seguridad de la información para los procesos académicos de la Universidad Nacional de Piura bajo el estándar NTP ISO/IEC. En este estudio se llevó a cabo el análisis de las vulnerabilidades y riesgos de los procesos involucrados y la propuesta de los controles de seguridad que se deben considerar.

En julio del 2020 en un trabajo desarrollado por la Universitaria Rafael Núñez de Colombia [33] , se diseñó un sistema de gestión de seguridad de la información para el proceso de gestión de la infraestructura tecnológica de instituciones académicas basado en la herramienta de gestión de riesgo Magerit. En este estudio se definió la importancia que tienen los activos en la institución, y se estableció que los activos de mayor relevancia para la organización por su impacto en los procesos administrativos y académicos son los servidores, los archivos de respaldo y seguridad, como también los mecanismos de accesos a los sistemas.

En la tabla 3 se resume las investigaciones referentes a auditorías, análisis de riesgos e implementación de Sistemas de Gestión de la Seguridad de la Información.

Tabla 3: Artículos sobre investigaciones de auditoría, análisis de riesgos e implementación de Sistemas de Gestión de la Seguridad

Lugar y fecha de publicación	Título del documento	Vulnerabilidades encontradas	Herramientas utilizadas	Metodología
Institución Educativa Departamental Luis Carlos Galán Colombia / octubre de 2017	Auditoria de seguridad informática para la Institución Educativa Departamental Luis Carlos Galán - Municipio de Yacopí Cundinamarca	puertos abiertos, fallos a nivel de sistemas operativos, aplicativos o servicios, vulnerabilidades tipo ransomware, alto riesgo de amenazas y vulneración en servidores web, denegaciones de un servicio, malas prácticas para la asignación de passwords.	Nmap, ping, Zenmap, Nessus y Nikto, John The Ripper.	Ethical hacking para el análisis de vulnerabilidades, Magerit V3 para el análisis de riesgos y análisis de riesgos y mejora continua PHVA (planificar, hacer, verificar, actuar) como lo recomienda la norma ISO/IEC 27001.
Universidad Estatal del Sur de Manabí / noviembre 2018.	Diseño de un modelo de gestión de seguridad de la información para el sistema académico de la Universidad Estatal del Sur de Manabí.	Borrado de información, limitado registro de equipos informáticos, posibilidad de infección con software de denegación de servicio.	ISO2701, ISO2702.	Metodología PDCA (Planificar - Hacer - Verificar - Actuar) en donde se establecen lineamientos de seguridad de la información en el sistema académico S@U basados en el estándar internacional ISO 27002:2017.
Universidad Nacional de Piura / julio 2019.	Diseño de un sistema de gestión de seguridad de la información para los procesos académicos de la Universidad Nacional de Piura. NTP ISO/IEC.	Errores en backups, falta de control de acceso, falta de control de trasporte o transferencia, ambiente inseguro, exceso de privilegios, ambiente inseguro, contraseñas inseguras, presencia de virus, falta de condiciones de seguridad, mantenimiento insuficiente.	ISO 17799. (ISO 17799, 2000) ISO/IEC 27002 CNB & INDECOPI, 2008.	Investigación aplicada y no experimental con información cuantitativa y cualitativa. Las técnicas usadas fueron: entrevistas, revisión documental, observaciones de campo y cuestionarios.
Año 2020/Corporación Universitaria Rafael Núñez / julio 2020.	Diseño de un sistema de gestión de seguridad de la información para el proceso de gestión de la infraestructura tecnológica de instituciones académicas basado en la herramienta de gestión de riesgo Magerit.	Importancia de los activos en la institución, su relevancia para la organización por su impacto en los procesos administrativos y académicos. Activos críticos son servidores, los archivos de respaldo y seguridad, y los mecanismos de acceso al sistema.	MAGERIT, MOVA.	Cuantitativa, con diseño no experimental transeccional descriptivo. Aplicación de un sistema de gestión adecuado a sus políticas, mediante el enfoque de la norma ISO 27001 y la metodología MAGERIT. Caracterización y ponderación de los activos, amenazas y salvaguardas. Mecanismos de control y políticas de seguridad.

Luego de revisar cada uno de los trabajos de investigación descritos, es preciso recalcar y diferenciar tres tipos de trabajos.

Dentro del primer grupo se encuentran aquellos estudios que están enfocados al análisis de vulnerabilidades de sistemas académicos que principalmente utilizan herramientas de gestión de seguridad como pruebas de penetración, Nmap, Nessus, Metasploit, WireShark, Owasp Zap, Nikto; la mayoría enfocadas en los estándares y normativas ISO/IEC. Los trabajos de investigación encontrados son hasta el 2021. En este año se presenta la pandemia la cual retrasa nuevas investigaciones sobre este tema.

El segundo grupo se centra en el análisis de vulnerabilidades WEB en donde se utilizan principalmente herramientas de hacking como NetCraft, Domain Tools, Nmap, SQLmap,

Owasp, Skipfish, entre otras. Los trabajos de investigación encontrados son hasta el 2020. En este año se presenta un mayor uso de aplicaciones móviles [34] y muchas instituciones empiezan a desarrollar aplicaciones en esta plataforma, por lo dedican más investigaciones de seguridad.

El tercer grupo se encuentran aquellas investigaciones de auditoría, análisis de riesgos y amenazas para proponer un sistema de gestión de seguridad de la información (SGSI) utilizando como herramienta principal la norma ISO/IEC 27001. A partir del 2020 sobresalen el uso de nuevas metodologías de riesgo como: NIST y MAGERIT.

La herramienta más actual para el análisis de vulnerabilidades es la aplicación del hacking ético que se basa en la metodología de ataque con los instrumentos de la suite de Kali Linux. Además, se debe considerar la norma de la familia ISO/IEC 27001 como referente de buenas prácticas y para la implementación de controles, no se puede dejar de lado la aplicación de otras metodologías como la PDCA y OWASP, que sirven de guía de referencia para llevar a cabo la determinación de vulnerabilidades dentro de un determinado sistema. La metodóloga de OWASP es la más utilizada en los últimos años.

Dentro del análisis de los trabajos investigados referente al análisis de vulnerabilidades de sistemas académicos, destaca el hacking ético mediante pentesting para la detección y análisis de vulnerabilidades en la red inalámbrica, realizado en la institución educativa de la provincia de Santa Elena. Este estudio es muy completo y detalla todos los procesos y subprocesos que se llevaron a cabo para detectar todas las debilidades referentes a la seguridad informática. En esta investigación se hace referencia al uso de herramientas de detección de fallas de seguridad como son: suite de Kali Linux, NMAP, Exposición Común CVE, Mitre-CVE, CVE-ID, VirtualBox, Metasploit, Ettercap, WireShark.

3 Materiales y metodología

3.1 Introducción

La Planificación del hacking ético se lleva a cabo considerando el estudio realizado al recopilar la información de casos exitosos de análisis de vulnerabilidades descritos en el desarrollo del estado del arte tratado anteriormente. En esta ocasión y después de revisar estudio nacional e internacional se llegó a definir que la metodología Estándar de Ejecución de Pruebas de Penetración (PTES) es el más adecuada para implementar el análisis de vulnerabilidades del sistema académico del Instituto Superior.

3.2 Estándar de Ejecución de Pruebas de Penetración (PTES)

El Estándar de Ejecución de Pruebas de Penetración con sus siglas en ingles PTES proporciona un conjunto de herramientas para la realización de un análisis completo de amenazas y vulnerabilidades e inseguridades de un sistema. Este modelo permite mediante una secuencia de 7 secciones cubrir por completo las pruebas relacionadas de penetración, desde recopilación de la información hasta la construcción final de un informe técnico para dar a conocer los hallazgos encontrados en temas referentes a la inseguridad de la información.

Las pruebas específicas de penetración cumplen con un estudio completo de amenazas y vulnerabilidades para posteriormente someter al sistema a un examen de penetración donde se evalúa la robustes del entorno ante eventuales eventos de inseguridad sociales y cibernéticos que se puedan suscitar. El nivel de detalle de un análisis varía según el entorno, donde cada organización define que área es más crítica y que desea proteger y es preciso aumentar la intensidad de pruebas en aquellas áreas donde más lo necesita.

Las 7 secciones del Estándar de Ejecución de Pruebas de Penetración son:

1. Interacciones previas al compromiso: Presentar y explicar las herramientas, métodos y técnicas disponibles que coadyuven al compromiso satisfactorio de las pruebas de penetración.
2. Recolección de información: Recabar toda la información posible sobre los objetivos que serán probados durante las pruebas de penetración.
3. Modelo de amenazas: Identificar los riesgos y las amenazas más probables, así como los bienes o activos que más debería resguardar.
4. Análisis de vulnerabilidades: Especificar posibles fallas de seguridad que puedan ser aprovechados por los ciber atacantes.
5. Explotación: Ejecutar pruebas de acceso a algún sistema o dispositivo aprovechando las fallas de seguridad encontradas en la fase anterior.

6. Post-Explotación: Analizar si conviene mantener este acceso para continuar avanzando dentro del entorno, para obtener información posteriormente o hacer actividades de monitoreo.
7. Informe: Reportar todo el proceso de pentesting a partir de la información recolectada, las fallas identificadas y explotadas y la información sensible obtenida.

3.3 Planificación del Hackeo Ético

Antes de iniciar con la planificación y desarrollo del hackeo ético es importante aclarar que desde este punto se hará referencia durante la redacción de este documento a dos servidores muy bien definidos. Se denominará servidor principal al recurso informático en donde se encuentra operando en sistema académico Fénix que actualmente se encuentra funcionando en el Instituto Superior. Por otro lado, se denominará servidor duplicado al recurso informático en donde se encuentra operando la copia del sistema académico Fénix que se utilizará para la realización de todas las pruebas de seguridad para llevar a cabo un eficiente análisis de vulnerabilidades que es uno de los objetivos de este trabajo de grado.

Para una correcta planificación del hackeo se ilustra en la tabla 4 los detalles de las 7 secciones que se aplicaran en el análisis de vulnerabilidades del sistema académico del Instituto Superior.

Tabla 4:Planificación de actividades a cumplir para el desarrollo de las 7 secciones del modelo PTES.

Análisis de Vulnerabilidades del Sistema Académico con PTES	
Secciones	**Actividades**
1. Interacciones previas al compromiso	• Autorización para poder realizar el análisis de vulnerabilidades al sistema académico • Solicitud de la copia del sistema académico Fénix dirigido al Rector del Instituto principal interesado. • Se realizará un respaldo completo del servidor y de la base de datos para el resguardo de la información previo a las pruebas de penetración en un servidor duplicado. • Oficio dirigido a la máxima autoridad del Instituto informando los por menores de las pruebas a realizar. • Firma de carta de confidencialidad
2. Recolección de información	• Recoger la información necesaria de los equipos, procesos, sistemas e interfaces comprometidas en análisis de seguridad de la información del sistema académico. • Encuesta acerca de las características del sistema académico dirigida a tres personas del departamento de TI y a tres personas externas. • Herramientas para reconocimiento pasiva: Whois, Netcraft, recon-ng, Nslookup.

3. Modelo de amenazas	• Definir los activos y procesos institucionales a proteger. • Especificar las características del atacante, comunidades de amenaza y agentes. • Ataques: DoS, SQL injection, y otros que guardan relación con los activos.
4. Análisis de vulnerabilidades	• Determinar adecuadamente la profundidad y amplitud aplicables a las pruebas. • Detallar las herramientas a utilizar y sus parámetros. • Pruebas activas, pasivas y su validación • Herramientas de análisis de vulnerabilidades: Fping, nmap, wireshark, openvas, metaexploit, armitage.
5. Explotación	• Tratar de acceder a un sistema o recurso eludiendo restricciones de seguridad. • Obtener información, dns, contraseñas, etc. • Periodo de ejecución de pruebas
6. Post-Explotación	• Reunir todos los hallazgos de seguridad encontrados junto con sus detalles
7. Reportes	• Resultados • Observaciones • Conclusiones • Hallazgos

Luego de la definición de las actividades para cada uno de las siete secciones que se deben considerar al implementar un análisis de vulnerabilidades con el Estándar de Ejecución de Pruebas de Penetración (PTES) es imprescindible considerar los requisitos necesarios para llevar a cabo tales tares. En este sentido se detalla a continuación un conjunto de equipos y sistemas a utilizar para el desarrollo del análisis.

Requerimientos de Hardware

- Servidor en donde se encuentra alojado el sistema académico Fenix.
- Servidor duplicado en donde se instalará la copia del sistema.
- Equipo de cómputo que se utilizara para las pruebas de análisis de vulnerabilidad.
- Comunicaciones necesarias

Requisitos de Software

- Aplicativo de sistema académico Fenix.
- Información del sistema operativo del servidor
- Base de datos del sistema académico

Otros requerimientos

- Usuario y contraseña de acceso administrativo al servidor.
- Acceso al respaldo de la base de datos del sistema académico.

Así mismo, se definen algunas consideraciones iniciales con el propósito de salvaguardar la integridad y el funcionamiento óptimo de los sistemas del Instituto. Por ningún motivo

se desea interferir en el trabajo diario de docentes y estudiantes. A continuación, se enlistan algunas consideraciones generales:

- ✓ Las pruebas de análisis de vulnerabilidades se desarrollarán en un respaldo del sistema original para resguardar el buen funcionamiento del sistema principal.
- ✓ No se alteran los recursos de comunicación de la institución.
- ✓ No se realizarán modificaciones, alteraciones o eliminaciones de archivos o documentos que pertenezcan a la institución.
- ✓ No se divulgarán los resultados obtenidos en las pruebas de análisis de vulnerabilidad.
- ✓ Se elaborará un informe de resultados en el cual se especifiquen los procesos llevados a cabo en el análisis de vulnerabilidades con sus respectivas recomendaciones.

Cronograma

El cronograma a seguir para la implementación del hacking Ético en el sistema académico Fénix del Instituto Superior se basa en los procesos a completar para cumplir con el estándar PTES. En este sentido se presenta un cronograma con fechas tentativas para efectuar estas tareas en la siguiente tabla 5.

Tabla 5: Detalles del cronograma para cumplir con las secciones del modelo PTES

Actividades	Octubre				Noviembre				Diciembre			
	1	2	3	4	1	2	3	4	1	2	3	4
Interacciones previas al compromiso			X	X								
Recolección de información			X	X								
Modelo de amenazas					X	X						
Análisis de vulnerabilidades						X	X	X	X			
Explotación								X	X			
Post-Explotación								X	X			
Reporte									X	X		

3.4 Desarrollo del hacking ético al sistema Fénix

En este apartado, se pretende detallar cada una de las secciones del Estándar PTES mencionadas anteriormente. La reglamentación constituyen una buena guía para llevar

a cabo de forma ordenada y sistémica el proceso de análisis de vulnerabilidades en el sistema académico del Instituto Superior.

3.4.1 Interacciones previas al compromiso

El Instituto Superior es una institución de educación superior publica en donde se enseña a las jóvenes pueden optar por carreras de nivel en las ramas de la ciencia y la tecnología. Para llevar a cabo los procesos internos los docentes y estudiantes de este establecimiento ha venido desarrollados programas informáticos que ayudan de manera considerable a automatizar, organizar y gestionar de manera significativa las tareas del sistema académico y los procesos de enseñanza - aprendizaje.

En el 2019 se desarrolla la versión más estable del sistema académico Fénix en donde intervienen docentes y estudiantes de la carrera de Tecnología Superior en Desarrollo de Software. Con este programa que actualmente funciona de forma efectiva, se pueden completar varias actividades docentes como el registro de notas, la generación de documentos académicos y muchos otros procesos.

Siendo el siguiente objetivo específico ejecutar la planificación del hackeo ético para el análisis de vulnerabilidades al sistema académico Fénix se redactó un documento en donde se solicita al principal interesado, el Rector del Instituto, un permiso para el acceso a la información del instituto y al sistema académico Fénix. Con este permiso se dispone de manera formal el consentimiento de indagar en el sistema mencionado; este documento se puede observar en el Anexo A. El Rector del Institutito Superior Tecnológico del Azuay respondió a esta solicitud de forma satisfactoria (Anexo B).

La licencia de funcionamiento y los derechos del sistema académico Fénix le pertenecen al Instituto Superior, por esta razón se mantuvieron algunas reuniones con las autoridades y desarrolladores para solicitar una copia de este sistema académico con el propósito principal de instalar este software en un servidor duplicado de similares características y así poder llevar a cabo las pruebas de análisis de vulnerabilidades en un ambiente controlado y seguro. La solicitud de estos recursos informáticos se puede ver en el Anexo C.

Posteriormente, se consideró la elaboración y firma de un documento jurídico en donde se establezcan algunos acuerdos en donde los solicitantes del software se comprometen a gestionar el buen uso del sistema académico, la responsabilidad de no ejecutar copias del mismo para su venta o comercialización y algunas prohibiciones adicionales. En los Anexos D1 y D2, correspondientes a Daniel Orellana y Fabián Chuqui respectivamente, se puede ver el detalle de este Compromiso de confidencialidad, no divulgación de la información y buen uso del software.

Así mismo, para una adecuada comunicación con las autoridades se redactó un oficio dirigido a la máxima autoridad del Instituto informando los pormenores de las pruebas a realizarse en la copia del sistema académico Fénix instalado en el servidor duplicado. Este documento se puede revisar en el Anexo E.

Cabe mencionar que en las interacciones previas al compromiso existió un cambio de autoridades, es decir al principio las solicitudes fueron dirigidos al Mgtr. Boris Chumbi que se encontraba como rector encargado hasta ese entonces, luego a partir de julio de 2022 se presentó la gestión de cambio de autoridad, actualmente es el Dr. Marcelo Aguilera el rector del Instituto Superior.

3.4.1.1 Recolección de información

Una vez que se nos autorizó y entregó la copia del sistema académico fénix del Instituto Superior se procedió a recolectar información acerca de las características técnicas del servidor principal para poder replicar esta configuración y posteriormente instalar la copia del sistema entregado.
Las características técnicas del servidor en donde actualmente se encuentra montado el sistema académico del Instituto son las que se muestra en la tabla 6:

Tabla 6: Características del servidor del Instituto Superior

Sistema Operativo	Ubuntu Server 18.04.4 LTS
Procesadores virtuales	8 Cores
Memoria Ram	16GB
Disco Duro	200GB

La información contenida en la tabla es relevante puesto que se dispondrá de un servidor duplicado de las mismas características para poder instalar la copia del sistema académico Fénix.

En este mismo proceso de recolección de información y como respuesta a la solicitud de la copia del sistema académico Fénix realizada en el apartado anterior se recibió de parte del departamento de TI los siguientes recursos informáticos.

- Copia de la base de datos (Docker del sistema académico Fénix)
- Código fuente del sistema académico Fénix
- Ejecutable del sistema académico Fénix

Para la configuración y levantamiento de estos recursos informáticos en el servidor duplicado es necesario cumplir con una serie de pasos los cuales se describen a continuación:

1. Instalación de Docker
2. Instalación de Postgress 11.7
3. Copia del código fuente y base de datos al servidor duplicado
4. Configuración de accesos del servidor duplicado
5. Configuración del Docker
6. Configuración de la base de datos
7. Configuración de accesos en el código fuente
8. Levantamiento del sistema académico

Una vez concluida la instalación y configuración del sistema académico Fénix en el servidor duplicado se realizan pruebas de funcionamiento para comprobar que los accesos y el buen funcionamiento del software sea óptimo. En la figura 1 se muestra el acceso satisfactorio al sistema instalado en el servidor duplicado.

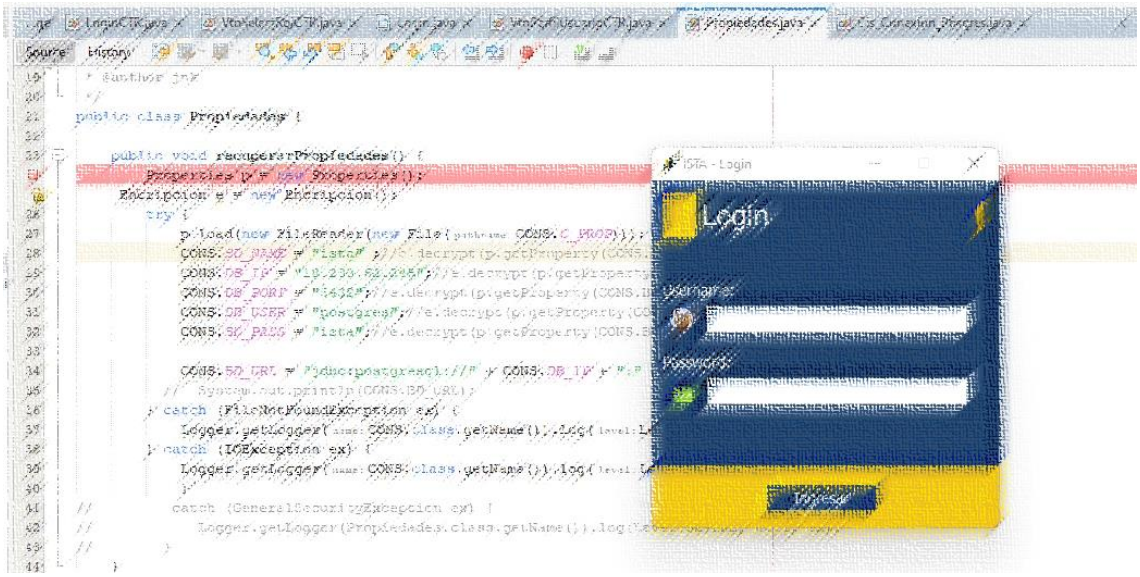


Figura 1:Acceso al sistema Fénix instalado en el servidor duplicado. Fuente: Propia.

Estos insumos serán imprescindibles para realizar el análisis de vulnerabilidades del sistema académico. Así mismo, se cuenta con una copia de cada una de las partes que conforman el Fénix instalados en el servidor duplicado en donde se puede extraer extensa información valiosa para el propósito de este trabajo.

Aplicación de herramientas de reconocimiento pasivo

En la búsqueda de información relacionada al sistema académico Fénix se procedió a la recopilación de información con la ayuda de las herramientas de reconocimiento pasivo que se maneja en la seguridad de la información. En este sentido se dispuso de herramientas como Whois, Netcraft, recon-ng y Nslookup para indagar en el sistema académico Fénix.

Para poder aplicar estas herramientas es necesario saber la dirección URL o la dirección IP que se utiliza para este servicio. Estos parámetros fueron identificados en el código fuente del sistema académico Fénix en donde en líneas de programación se obtuvo la dirección del servidor y otros datos para llevar a cabo las pruebas. Por razones de confidencialidad no se colocará este dato de forma legible en la fase de reconocimiento pasivo.

Tabla 7: Detalles ocultos de las direcciones electrónicas del servidor principal y duplicado.

Dirección URL del servidor principal del sistema Fénix del Instituto.	Dirección URL del servidor duplicado donde se instaló la copia del Fénix.

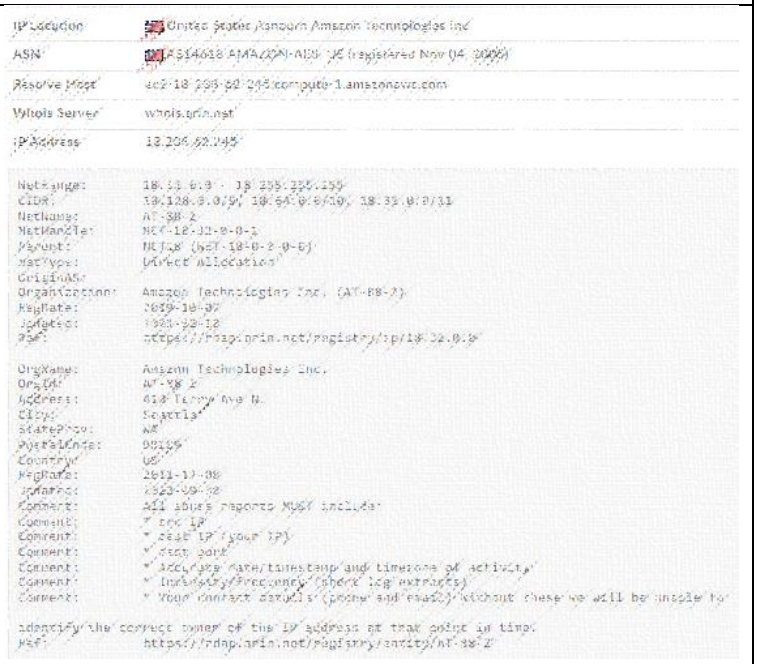
xxxxxx.xxxxxxxxx.edu.ec	xxxxxxxx.xxxxxxxx.xxx.com

Los resultados mostrados en la tabla 7 se obtuvo al aplicar estas herramientas en la fase de recopilación de información se describen a continuación

Whois

La herramienta proporciona el servicio de búsqueda de dominios el cual integra un directorio gratuito y de acceso público con los detalles de la información técnica y los registros de los titulares del dominio registrado. En este sentido si se hace uso de este recurso informático se obtiene la información que se muestra en la tabla.

Tabla 8: Detalles del análisis de dominios para el servidor principal y el duplicado con la herramienta whois

Servidor principal	Servidor duplicado
	

Como se observa, los resultados obtenidos con Whois no son tan precisos y hacen referencia a un servidor que se encuentra en la ciudad de Illinois Chicago en el país de los Estados Unidos. En consecuencia, lo que se está identificando en este caso es el servidor en donde se encuentra alojado el sitio web más no el sistema académico Fénix.

Dnsdumpster

Esta herramienta web entrega buenos resultados e identifica una dirección IP local que pertenece a una institución de educación que se encuentra estrechamente relacionada a los parámetros definidos en el sistema académico Fénix.

Por razones de seguridad se ocultarán los resultados obtenidos.

Tabla 9: Resultados del análisis de dominios para el servidor principal como para el duplicado.

Servidor principal	
Servidor duplicado	

Con la herramienta dnsdumper se encontró efectivamente las direcciones IP asociadas al servidor principal y al servidor duplicado. Con estos datos se podrá hacer uso de otras herramientas de reconocimiento pasivo como las que se analizarán a continuación

Robtex

Esta herramienta actualmente una de las herramientas más manejadas a nivel mundial para poder examinar y extraer información de los dominios. Con Robtex se realiza una inspección de las direcciones IP encontradas tanto del servidor principal como del servidor duplicado. A continuación, se muestran los resultados obtenidos con este utilitario.

Tabla 10: Detalles del análisis de dominios con la herramienta Robtex.

Servidor principal	Servidor duplicado
	

Como indican los resultados, el servidor principal se encuentra alojado en las instalaciones del Universidad de Cuenca, es decir que la base de datos del sistema académico Fénix está alojado en un servidor de esta institución. Por otro lado, se puede

observar que el servidor virtual duplicado se encuentra en la Compañía General Electric en Fairfield Estados Unidos.

Dnsrecon

DNSRecon es una herramienta de escaneo y enumeración DNS escrita en Python, la cual permite realizar diferentes tareas, como enumeración de registros estándar para un dominio definido (A, NS, SOA y MX). En esta ocasión se utiliza esta herramienta para conocer las direcciones asociadas al servidor principal y al servidor duplicado del sistema académico Fénix.

Tabla 11: Detalles del análisis de dominios del servidor principal y duplicado con dnsrecon

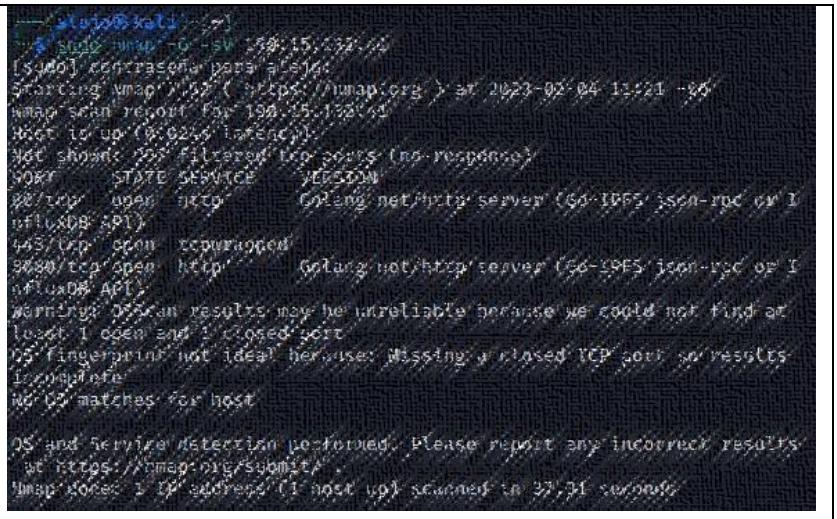
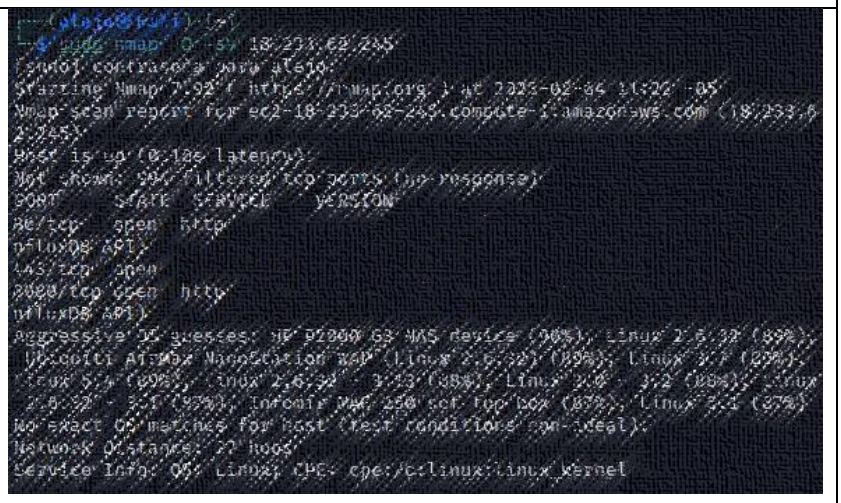
Servidor principal	
Servidor duplicado	

Nmap

La herramienta de análisis de red y seguridad Nmap es muy versátil, integra muchos parámetros que se pueden configurar para realizar consultas de distintas maneras y obtener resultados según los parámetros establecidos.

En este caso se utilizará Nmap para obtener información de los puertos del servidor principal y del servidor duplicado. Los resultados obtenidos se muestran a continuación.

Tabla 12: Análisis de puertos del servidor principal y duplicado con Nmap.

Servidor Principal	
Servidor duplicado	

Con la ayuda de la herramienta de reconocimiento pasivo se encontraron los siguientes datos:

Tabla 13: Resumen de hallazgos encontrados en el análisis de puertos con Nmap

Servidor Principal	Servidor duplicado
• Red del servidor: CEDIA • País: Ecuador • Sistema operativo: Linux. • Protocolos en servicio: Golang net/http server (Go-IPFS json-rpc or InfluxDB API) • Puertos usados: 80, 8008 y 8080. • Sistema operativo: Linux	• Red del servidor: AMAZON-AES • País: Estados Unidos • Protocolos en servicio: 80/desconocido/TCP, 8008/HTTP/TCP y 8080/desconocido/TCP. • Puertos usados: 80, 8008 y 8080. • Sistema operativo: Linux

3.4.2 Modelo de amenazas

En el modelo de amenaza se identifican amenazas y riesgos más probables, así como los bienes o activos que más debería resguardar. A continuación, se establecen el análisis de estos parámetros para establecer el modelo de amenaza.

Activos institucionales a proteger

Para el hackeo ético que contempla el análisis de vulnerabilidades del sistema académico Fénix, es necesario identificar de forma correcta todos lo activos que participan de una u otra manera en el uso cotidiano del este sistema. En conveniente en este punto mencionar que solo los docentes y personal administrativo tienen acceso al Fénix.

En la tabla 14 se exponen los principales activos que intervienen en el buen funcionamiento del sistema académico.

Tabla 14: Activos de información relacionados al sistema Fénix

Categoría	Subcategoría	Activo	Código	Físico / Digital	Ubicación
Activos esenciales	Información	Calificaciones	EI1	Digital	DB Fénix / Postgres / dbphoenix.tecazuay.edu.ec /CEDIA / Universidad de Cuenca
		Matrículas	EI2	Digital	
		Inscripciones	EI3	Digital	
		Asignaturas	EI4	Digital	
	Datos personales	Datos personales de estudiantes	ED1	Digital	DB Fénix / Postgres / dbphoenix.tecazuay.edu.ec /CEDIA / Universidad de Cuenca
		Datos personales de estudiantes	ED2	Digital	
	Servicios	Fénix	ES1	Digital	DB Fénix / Postgres / dbphoenix.tecazuay.edu.ec /CEDIA / Universidad de Cuenca
Datos / Información	Respaldos	Respaldos de la base de datos	DR1	Digital	DB Fénix / Postgres / dbphoenix.tecazuay.edu.ec /CEDIA / Universidad de Cuenca
	Credenciales	Usuarios	DC1	Digital	
		Contraseñas	DC2	Digital	

Claves criptográficas	Protección de accesos	Cifrado MD5	KP1	Digital	DB Fénix / Postgres / dbphoenix.tecazuay.edu.ec /CEDIA / Universidad de Cuenca
Software	Servidor de ficheros	Base de datos del Fénix	SS1	Digital	Servidor dbphoenix.tecazuay.edu.ec /CEDIA / Universidad de Cuenca
	Gestión de Bases de datos	Gestor de Base de datos del Fénix	SS2	Digital	Servidor dbphoenix.tecazuay.edu.ec /CEDIA / Universidad de Cuenca
	Sistema de respaldos	Sistema de respaldo del Fénix	SS3	Digital	Computadora del Jefe de TIC / Instituto del Azuay
	Programas	Programa ejecutable del sistema Fénix	SS4	Digital	Computadoras de personal del Instituto del Azuay
Equipos físicos	Computadores personales de usuarios	Computadores de docentes	EP1	Físico	Computadores de los docentes del Instituto del Azuay
		Computadores de administrativos	EP2	Físico	Computadores del personal administrativo del Instituto del Azuay
	Equipos de red	Conmutador principal	ER1	Físico	Router principal/ Cuarto de equipos del Instituto del Azuay
		Encaminadores	ER2	Físico	Cuarto de equipos del Instituto
		Accesos inalámbricos	ER3	Físico	Cuarto de equipos del Instituto
	Servidores	Servidor del sistema Fénix	ER4	Físico	Servidor dbphoenix.tecazuay.edu.ec /CEDIA / Universidad de Cuenca
Redes de comunicación	Red inalámbrica	Red inalámbrica interna para docentes y administrativos	RC1	Físico	Equipos inalámbricos Access Point del Instituto del Azuay

	Red cableada	Red cableada interna para docentes y administrativos	RC2	Físico	Cableado UTP
	Internet	Red de internet para docentes y administrativos	RC3	Físico	Router de Fibra Óptica del Proveedor de Servicio de Internet
Personal	Usuarios	Internos	PU1	Físico	Comunidad del Instituto del Azuay
		Externos	PU2	Físico	Personal externos (organizaciones, empresas, proveedores, unidades educativas)

Como se puede observar en la tabla, se ha podido identificar un total de 26 activos asociados al uso del sistema académico Fénix. Con esta lista, se puede analizar de mejor manera las cualidades que deben tener los potenciales atacantes y demás personas que quieran someter al sistema.

Procesos institucionales a proteger

Con respecto a los procesos que se manejan a través del sistema académico Fénix del Instituto Superior es preciso indicar que los docentes y personal administrativo acceden al Fénix para desarrollar y cumplir con distintos procesos entre los cuales podemos destacar la elaboración de documentos académicos, registro de notas, registro de matrículas, inscripciones, comprobantes, entre otros. A continuación, se enlista los procesos que se encuentran dentro del sistema académico Fénix y que se desean proteger.

- Consultas
  - Información personal de la comunidad.
  - Especificaciones de periodos académicos.
  - Detalles de carreras, asignaturas y horarios.
  - Datos de matrículas.
  - Estudiantes matriculados, retirados y desertores.
  - Documentos académicos como sílabos, planes de clase, avances de sílabo.
  - Registros de notas parciales y finales.
  - Asistencia de los estudiantes.
  - Base de datos de la biblioteca.
- Ingreso de datos
  - Ingreso de información personal de la comunidad
  - Ingreso de datos de inscripciones

- Ingreso de datos de matrículas
    - Ingreso de roles y usuarios
    - Comprobantes de pago.
- Reportes
    - Número de alumnos
    - Fichas

Es importante indicar que estos procesos son gestionados por los docentes y administradores del Instituto Tecnológico del Azuay para cumplir con todos los procesos académicos que se realizan al inicio, durante y al finalizar cada periodo académico.

Características del atacante, comunidades de amenaza y agentes.

Los grupos organizados y personas que desean explotar las vulnerabilidades del sistema académico Fénix e ingresar de forma indebida a los recursos del Instituto podrían ser individuos que busquen distintos objetivos. Con base en el análisis que se realizó en el estudio del estado del arte y el análisis bibliográfico se determinaron los siguientes posibles ataques:

- Robo de información personal de estudiantes, docentes y administrativos
- Manipulación de calificaciones de los estudiantes
- Cambiar de paralelo o nivel a estudiantes
- Ingresar estudiantes no matriculados al sistema
- Borrar matriculas de estudiantes
- Cambiar registros de asistencia de estudiantes
- Manipular documentos académicos
- Modificaciones de perfiles de docentes y estudiantes
- Cambio de datos en comprobantes de pago
- Cambio de roles de usuarios

Con este panorama se espera que los atacantes tengan un perfil asociado a personas o grupos de individuos que tengan la intensión de beneficiar a estudiantes modificando datos académicos o perjudicar de una u otra forma al Instituto Superior siendo un establecimiento de educación superior que maneja distintos procesos para completar el proceso de enseñanza – aprendizaje de sus estudiantes.

Otro de los ataques que se pueden suscitar para tratar de ingresar al sistema académico está relacionado con la ingeniería social. En este caso las personas son generalmente el eslabón más débil de una empresa cuando se trata de la protección informática y ciberseguridad. Son 70 docentes y 5 personas que trabajan en el área administrativa por lo que se debe considerar un nivel de proteger adecuado para este importante activo de seguridad de la información.

Descripción de ataques

Los ataques que se pueden implementar al sistema académico Fenix se encuentran estrechamente relacionados a los activos de seguridad de la información asociados al sistema. En este sentido y luego de un análisis bibliográfico contemplado en el capítulo anterior se identifican algunos ataques puntuales que se pueden desarrollar al momento de intentar penetrar en el sistema académico Fénix. Es necesario mencionar que estos ataques ya se han presentado y documentado en acontecimientos pasados de inseguridad alrededor del mundo en ciberataques relacionados a sistemas informáticos. A continuación, se presentan los principales ataques que se pueden esperar en el sistema académico Fénix.

Ataque DoS

Es posible que un ataque DoS al sistema académico Fénix pueda ser implementado por un grupo de personas mal intencionadas. Estos atacantes realizar peticiones simultaneas y en masa al Fénix provocando que este colapse o se bloquee.

SQL injection

El sistema académico Fénix dispone de una base de datos amplia en donde se guardan todos los datos académicos y administrativos del Instituto Superior es por esta razón que un ataque SQL injection es posible que se pueda presentar ocasionando robo, manipulación o destrucción de la información

Ingeniería Social

Un ataque de ingeniería social es posible que se presente en cualquier momento debido a que los docentes del Instituto no han recibido cursos de capacitación y/o concienciación de este tipo de estafas. Así mismo, los docentes han adquirido un exceso de confianza entre la comunidad académica lo que facilita este tipo de amenaza informática.

Ataques de fuerza bruta

Este tipo de ataques consiste en realizar un numero alto de intentos por ingresar al sistema utilizando palabras comunes en el registro de usuario y contraseña. En el instituto no se dispone de un directorio activo ni de una política para el manejo de claves de acceso es por esta razón que un ataque de estos tendría éxito.

Phishing

Anteriormente se indicó que los docentes del Instituto no han recibido capacitaciones en temas de seguridad de la información y las amenazas a las que todas las organizaciones están expuestas, es por esta razón que un ataque de phishing se debe considerar probable. Por medio de enlace sospechosos de correos electrónicos o sitios fraudulentos los atacantes pueden abrir una vía de acceso al sistema académico.

Malware

Una navegación insegura e irresponsable por sitios fraudulentos puede llegar a infectar una o varias computadoras de docentes o administrativos del instituto provocando que tales equipos queden expuestos muchas veces a merced de los atacantes para que el acceso indebido o no autorizado sea realizado de forma satisfactoria.

Los ataques contemplados anteriormente no son todos los que existen, pero si son los que pueden llegar a afectar de forma más significativa al software académico Fénix, es por esto que se debe considerar principalmente estas posibles agresiones cibernéticas en la protección y defensa de los recursos que se integran al sistema académico del Instituto.

3.4.3 Análisis de vulnerabilidades

Los riesgos de la información están presentes cuando confluyen dos elementos bien definidos y asociados entre sí: las amenazas y vulnerabilidades. En este apartado se pretende realizar un análisis completo de las vulnerabilidades del Sistema Académico Fénix identificando sus componentes, sucesos, hitos, acciones, configuraciones y demás elementos que presentan una debilidad al momento de hacer frente a un ciberataque. A continuación, se especifican posibles fallas de seguridad que puedan ser aprovechados por los ciber atacantes

Profundidad y amplitud de las pruebas

En el capítulo anterior en donde se revisó el estado del arte referente a los casos más exitosos de análisis de vulnerabilidades se identificaron las metodologías de estos estudios. Estos detalles serán tomados en cuenta para definir la profundidad y amplitud de las pruebas a realizar en el sistema académico Fénix.

Al tener instalado este sistema en un servidor duplicado se cuenta con un ambiente controlado apto para realizar ciertas pruebas más rigurosas que no se pudieran implementar si estuviéramos trabajando en la propia institución con el Fénix dando servicio constante. Es por esta razón que se pretende realizar pruebas de hacheo ético, pentesting, y explotación del sistema a fin de obtener resultados de la vulnerabilidad del sistema académico ante estos posibles eventos de ciberataque.

A continuación, se describen las pruebas de seguridad de la información que se van a implementar en el sistema académico Fénix del Instituto Superior.

1. Pruebas para el análisis de las vulnerabilidades del código fuente del sistema.
2. Pruebas para el análisis de las vulnerabilidades del sistema Fénix.
3. Pruebas para el análisis de las vulnerabilidades de los usuarios.

Es importante definir para una mejor comprensión de la profundidad y amplitud de las pruebas de vulnerabilidades del sistema académico aquellos elementos que no se contemplan para este estudio. En este sentido es necesario indicar que el análisis de las vulnerabilidades en la red de comunicación no serán parte de estas pruebas de seguridad.

Con el afán de completar de forma satisfactoria las pruebas de análisis de vulnerabilidad se utilizarán algunas herramientas contempladas en el estudio de la seguridad de la información que se describen en el siguiente apartado.

Detalles de las herramientas y recursos a utilizar.

Para desarrollar las pruebas de análisis de vulnerabilidad en el sistema académico Fénix de forma satisfactoria es preciso definir las herramientas que se utilizarán. En este caso se contempla aprovechar la tecnología y los instrumentos de análisis para obtener resultados precisos y concretos.

A continuación, se enlistan las herramientas utilizadas para llevar a cabo cada una de las pruebas de análisis de vulnerabilidades:

Tabla 15:Lista de herramientas de seguridad que se usarán para el análisis de vulnerabilidades

Propósito de la herramienta o recurso	Herramienta / Recurso	Detalle de la herramienta o recurso
Análisis de vulnerabilidades del código fuente del sistema	Sonarqube	Herramienta que permite el desarrollo de análisis estático de código fuente.
	OWASP Dedendency Check	Herramienta que permite identificar las dependencias de un proyecto y comprobar si son susceptibles a vulnerabilidades conocidas.
Análisis de las vulnerabilidades del sistema Fénix (Accesos y Base de datos)	Nmap	Programa de código abierto que sirve para efectuar rastreo de puertos
	Nessus	Programa de escaneo de vulnerabilidades muy versátil aplicable a distintos sistemas.
Análisis de las vulnerabilidades de los usuarios	Ingeniería social (varias técnicas)	Práctica ilegítima de obtener información confidencial a través de la manipulación de usuarios

Es sustancial mencionar que el uso de las herramientas de análisis de seguridad será implementado en la copia del sistema académico Fénix instalado en el servidor duplicado constituyendo un ambiente controlado y seguro de trabajo.

A continuación, se describen los distintos análisis de vulnerabilidades aplicados al sistema académico Fénix.

3.4.3.1 Análisis de vulnerabilidades del código fuente del sistema

La primera herramienta que se va a utilizar para el análisis completo y automático de vulnerabilidades en el sistema es **SonarQube**. Este aplicativo es una herramienta que permite el desarrollo de análisis estático de código fuente identificando puntos susceptibles de mejora, para facilitar la obtención de métricas necesarias para la optimización del código.

Además, SonarQube es una plataforma de código abierto que se encarga de realizar una inspección continua de la calidad del código con la ayuda de distintas herramientas de análisis estático. Dentro de sus características integra herramienta esencial para realizar pruebas de funcionamiento y auditoría de código dentro del ciclo de desarrollo de una aplicación

El lenguaje de programación con el que fue desarrollado SonarQube es Java y permite analizar código entre 29 lenguajes de programación importantes, incluidos c / c ++, PL / SQL, Cobol, Jave, Java-Script, Php, entre otros, a través de conjuntos de reglas y varios complementos.

El resumen de resultados del análisis de vulnerabilidades del código fuente del sistema Fénix con la ayuda de SonarQube se muestra a continuación.

Tabla 16: Resumen de resultados entregados por la herramienta SonarQube

Resumen de vulnerabilidades del código fuente del Sistema Fénix

Métrica	Valor total	Categoría	Valor por categoría
Anomalías de código	85	Blocker	8
		Critical	0
		Major	70
		Minor	7
		Info	0
Vulnerabilidades	4	Blocker	2
		Critical	2
		Major	0
		Minor	0
		Info	0
Código sucio	6,2k	Blocker	3
		Critical	1,6k
		Major	1,1k
		Minor	3,3k
		Info	82
Puntos de acceso	7	HIGH (Autentication)	2
		MEDIUM (DoS)	3
		LOW Configuración insegura	1
		Otros	1

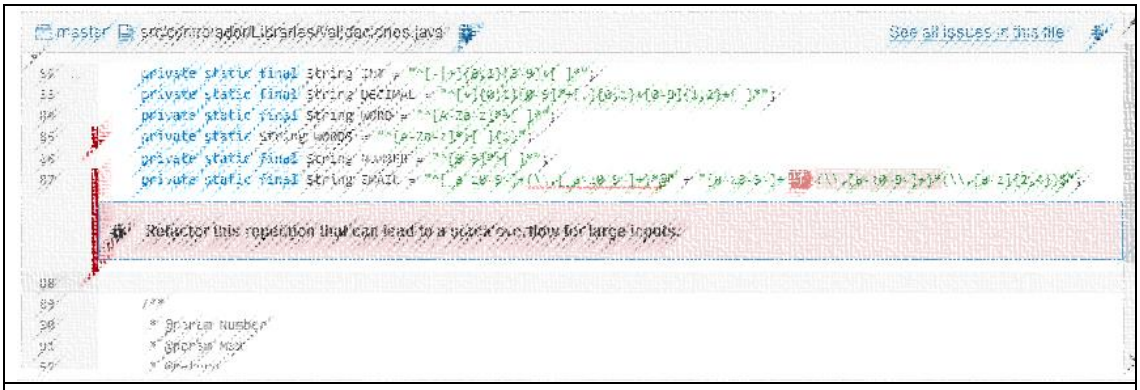
Como se puede observar existen varios inconvenientes de seguridad en el código del sistema académico Fénix según el análisis autónomo realizado por SonarQube. Cabe indicar que este estudio entrega como resultado las inseguridades en donde se puede observar el tipo de hallazgo, su criticidad y otros detalles como la porción de código con escritura deficiente y una propuesta de solución.

Es por eso que la herramienta de SonarQube es una de las mejores al momento de realizar análisis de código fuente.

Entre los hallazgos encontrados con nivel de criticidad alto se indican los siguientes

Tabla 17: Evidencias de algunas vulnerabilidades encontradas por SonarQube

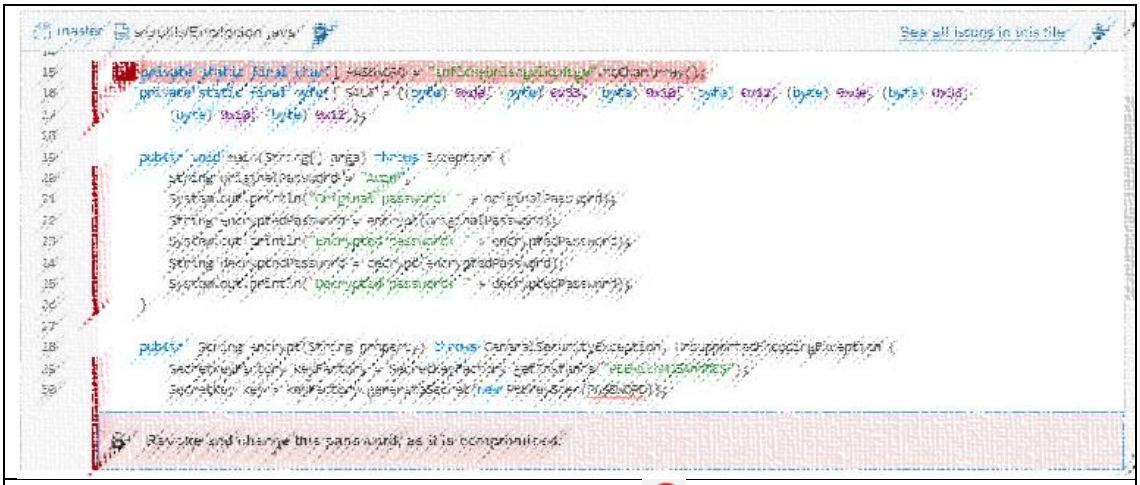
Anomalías de código
Refactorice esta repetición que puede conducir a un desbordamiento de pila para entradas grandes (Mayor)



Vuelva a interrumpir este método o vuelva a lanzar la "Excepción interrumpida" que se puede capturar aquí. (Mayor)

Llame a "xxxxxxxx#xxxxxxxxxx()" antes de acceder al valor. (Mayor)

Vulnerabilidades
Revoque y cambie esta contraseña, por lo que está comprometida. (Bloqueada)

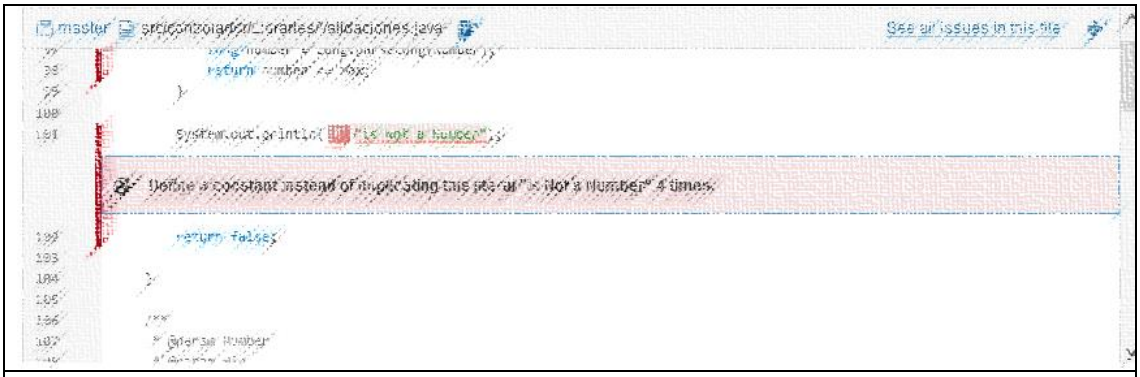


Utilice el modo seguro y el esquema de relleno. (Crítica)

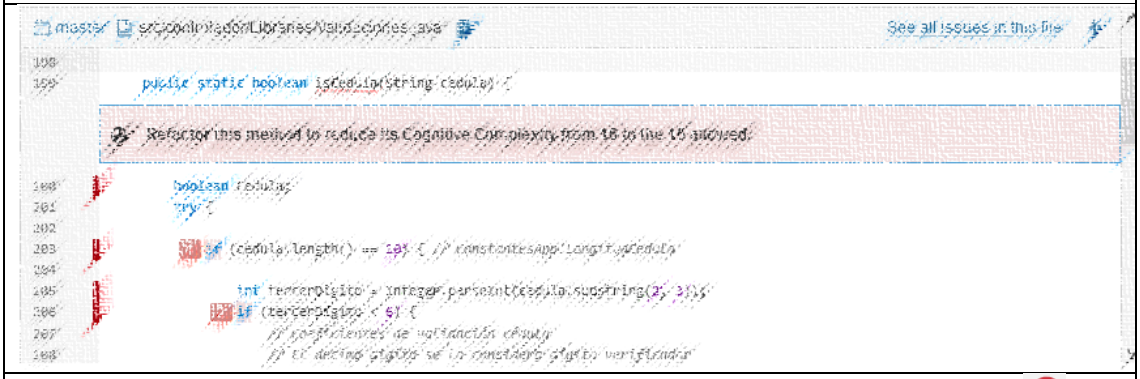
Utilice el modo seguro y el esquema de relleno. (Crítica)

Código sucio

Defina una constante en lugar de duplicar este literal "no es un número" 4 veces. (Crítica)



Refactorice este método para reducir su Complejidad Cognitiva de 16 a los 15 permitidos. (Crítica)

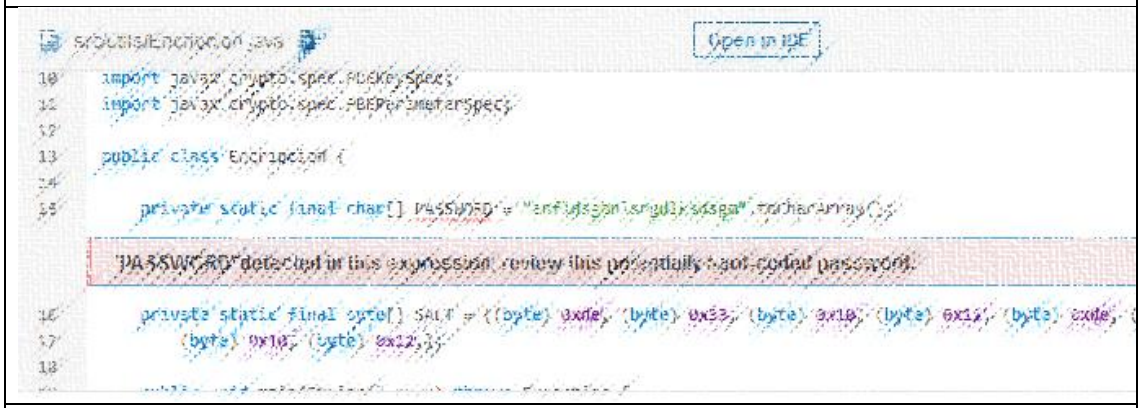


Defina una constante en lugar de duplicar este literal "Ver materias" 4 veces. (Crítica)

Puntos de acceso

'XXXXXXXXXX' detectada en esta expresión, revise esta contraseña potencialmente codificada. HIGH

'XXXXXXXXXX' detectada en esta expresión, revise esta contraseña potencialmente codificada. **HIGH**



Asegúrese de que las expresiones regular utilizada aquí, que es vulnerable al tiempo de ejecución polinomial debido al retroceso, no pueda provocar una denegación de servicio. **MEDIUM**

Los resultados del análisis de vulnerabilidades presentados por la herramienta de SonarQube hacen referencia a varias anomalías de código, aplicación de peticiones incorrectas, deficiente gestión de métodos, valores inseguros de código, uso de contraseñas encriptadas en texto plano, deficiente uso de modos seguros y esquema de relleno, así como también un número considerable de líneas de código sucio. (Code Smell).

Code Smell hace referencia al uso de síntomas en el código que indican la posibilidad de una forma incorrecta de programación, lo que puede ocasionar que haya algún problema a futuro y un problema de trasfondo.

Otro de los detalles que ofrece la herramienta SonarQube se indica en la siguiente tabla

Tabla 18: Resultados secundarios del análisis de vulnerabilidades de SonarQube.

Hallazgos secundarios en el código de Fénix	
Líneas duplicadas	4357
Bloques duplicados	266
Archivos duplicados	86

Otra de las pruebas de vulnerabilidad que se llevó a cabo se trata de un análisis de dependencias que consiste en estudiar las librerías que se utiliza en la programación de código. Este estudio investiga la aplicación correcta de insumos de desarrollo de software y su versión. Es imprescindible que las herramientas para el desarrollo del sistema Fénix se encuentren actualizadas. Para este análisis se dispone de la herramienta gratuita denominada **OWASP Dependency Check**.

El resumen de resultados que se obtuvieron en la aplicación de la herramienta de OWASP aplicada en el sistema de calificaciones Fénix es el siguiente:

Tabla 19: Resumen de vulnerabilidades encontradas con la herramienta OWASP Dependency-Check


Dependency-Check Report

DEPENDENCY-CHECK

Project: dependency-check scan /home/alejo/Escritorio/Sys-IST/Escritorio

Dependency	Vulnerability Ids	Package	Highest Severity	CVE Count	Confidence	Evidence Count
commons-beanutils-1.8.0.jar	cpe:2.3:a:apache:commons_beanutils:1.8.0:*	pkg:maven/commons-beanutils/commons-beanutils@1.8.0	HIGH	2	Highest	105
commons-beanutils-1.8.2.jar	cpe:2.3:a:apache:commons_beanutils:1.8.2:*	pkg:maven/commons-beanutils/commons-	HIGH	2	Highest	109
commons-collections-2.1.1.jar	cpe:2.3:a:apache:commons_collections:2.1.1:*	pkg:maven/commons-collections/commons-	HIGH	1	Highest	28
commons-collections-3.2.1.jar	cpe:2.3:a:apache:commons_collections:3.2.1:*	pkg:maven/commons-collections/commons-	HIGH	1	Highest	79

commons.jar	cpe:2.3:a:gradle:commons_net:1.0:-:-:-:-:-:-:-		MEDIUM	1	Low	24
groovy-2.4.7.jar	cpe:2.3:a:apache:groovy:2.4.7:*:*:*:*:*:*:*	pkg:maven/org.codehaus.groovy/groovy	CRITICAL	2	High	279
groovy-all-1.7.5.jar	cpe:2.3:a:kay_framework_project:kay_framework:1.7.5:*:*:*:*:*:*:*	pkg:maven/org.codehaus.groovy/groovy	CRITICAL	2	Low	258
groovy-all-2.0.1.jar	cpe:2.3:a:apache:groovy:2.0.1:*:*:*:*:*:*:*	pkg:maven/org.codehaus.groovy/groovy-all@2.0.1	CRITICAL	3	Highest	265
groovy-all.jar	cpe:2.3:a:apache:groovy:2.4.5:*:*:*:*:*:*:*		CRITICAL	2	High	55
groovy-ant.jar	cpe:2.3:a:apache:ant:2.5.2:*:*:*:*:*:*:* cpe:2.3:a:apache:groovy:2.5.2:*:*:*:*:*:*:*	pkg:maven/org.codehaus.groovy/groovy	MEDIUM	1	High	250
groovy.jar	cpe:2.3:a:apache:groovy:2.2.2:*:*:*:*:*:*:*	pkg:maven/org.codehaus.groovy/groovy	MEDIUM	1	Highest	292
itextpdf-5.5.9.jar	cpe:2.3:a:itextpdf:itext:5.5.9:*:*:*:*:*:*:*	pkg:maven/com.itextpdf/itextpdf@5.5.9	HIGH	3	High	84
jasperreports-6.3.0.jar	cpe:2.3:a:tibco:jasperreports_library:6.3.0:*:*:*:*:*:*:*	pkg:maven/net.sf.jasperreports/jasperreports	HIGH	8	Highest	45
jasperreports-6.5.1.jar	cpe:2.3:a:tibco:jasperreports_library:6.5.1:*:*:*:*:*:*:*		HIGH	2	High	25
jasperreports-fonts-6.1.1.jar	cpe:2.3:a:jaspersoft:jasperreports:6.1.1:*:*:*:*:*:*:* cpe:2.3:a:tibco:jasperreports_library:6.1.1:*:*:*:*:*:*:*	pkg:maven/net.sf.jasperreports/jasperreports-fonts	HIGH	4	Medium	28
junit-4.12.jar	cpe:2.3:a:junit:junit4:4.12:*:*:*:*:*:*:*	pkg:maven/junit/junit@4.12	MEDIUM	1	Low	24
log4j-1.2.17.jar	cpe:2.3:a:apache:log4j:1.2.17:*:*:*:*:*:*:*	pkg:maven/log4j/log4j@1.2.17	CRITICAL	6	Highest	29
mysql-connector-java-5.1.23.jar	cpe:2.3:a:mysql:mysql:5.1.23:*:*:*:*:*:*:* cpe:2.3:a:oracle:connector/j:5.1.23:*:*:*:*:*:*:*		CRITICAL	74	High	26
org.apache.commons.logging.jar	cpe:2.3:a:apache:commons_net:1.1.1:*:*:*:*:*:*:*		MEDIUM	1	Low	20
org.apache.commons.logging.jar	cpe:2.3:a:apache:commons_net:1.1.1:*:*:*:*:*:*:*		MEDIUM	1	Highest	17
poi-3.10-FINAL.jar	cpe:2.3:a:apache:poi:3.10:*:*:*:*:*:*:*	pkg:maven/org.apache.poi/poi@3.10-FINAL	HIGH	8	Highest	32
poi-3.17.jar	cpe:2.3:a:apache:poi:3.17:*:*:*:*:*:*:*	pkg:maven/org.apache.poi/poi@3.17	MEDIUM	2	Highest	33
poi-3.7-20101029.jar	cpe:2.3:a:apache:poi:3.7:*:*:*:*:*:*:*	pkg:maven/org.apache.poi/poi@3.7	HIGH	9	Highest	35
poi-3.9-20130515.jar	cpe:2.3:a:apache:poi:3.9:20130515:*:*:*:*:*:*	pkg:maven/com.haulmont.thirdparty/poi@3.9-20130515	HIGH	7	Highest	36
postgresql-42.2.5.jar	cpe:2.3:a:postgresql:postgresql_jdbc_driver:42.2.5:*:*:*:*:*:*:*	pkg:maven/org.postgresql/postgresql@42.2.5	CRITICAL	5	Low	47
postgresql-9.4.1209.jar	cpe:2.3:a:postgresql:postgresql_jdbc_driver:9.4.1209:*:*:*:*:*:*:*	pkg:maven/org.postgresql/postgresql@9.4.1209	CRITICAL	5	Low	46
postgresql-9.4.1212.jar	cpe:2.3:a:postgresql:postgresql_jdbc_driver:9.4.1212:*:*:*:*:*:*:*	pkg:maven/org.postgresql/postgresql@9.4.1212	CRITICAL	5	Low	45
spring-build-src-4.0.1.RELEASE.jar	cpe:2.3:a:gradle:gradle:4.0.1:release:*:*:*:*:*:*		CRITICAL	7	Low	9
spring-build-src-4.0.1.RELEASE.jar	cpe:2.3:a:gradle:gradle:4.0.1:release:*:*:*:*:*:*		CRITICAL	7	Low	9
spring-core-4.0.1.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_framework:4.0.1:release:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:4.0.1:release:*:*:*:*:*:*	pkg:maven/org.springframework/spring-core@4.0.1.RELEASE	CRITICAL	16	Highest	33

La tabla resumen de resultados del análisis de dependencias con OWASP Dependency Check muestra 18 vulnerabilidades críticas, 11 mayores y 11 medias. Estos parámetros merecen ser atendidos de urgencia puesto que significa una debilidad significativa para el código fuente y por consecuencia para el sistema Fénix.

Los hallazgos identificados por esta herramienta están relacionados en su mayoría a desactualizaciones en las librerías que utilizan en el código fuente y en el desarrollo de la aplicación Fénix. Es por esto que se detectan como potenciales vulnerabilidades y al tratarse de una clasificación critica de estos indicadores se debe brindar una solución oportuna.

Al trabajar con librerías o dependencias de programación caducadas es muy conveniente por temas de seguridad actualizar estos recursos. La mayoría de ataques de diferentes tipos se ocasionan por la falta de parches de seguridad que se obtienen actualizando los complementos y sistemas de información y programación.

3.4.3.2 Análisis de las vulnerabilidades del sistema Fénix

El análisis de vulnerabilidades del sistema académico Fénix comienza con la aplicación de los procesos de análisis que ofrece la herramienta de seguridad de la información **Nmap**. En este caso se utiliza este recurso para obtener información de los puertos del servidor principal en donde se encuentra instalado el sistema Fénix.

Para llevar a cabo este análisis de puertos se utiliza la herramienta nmap con el parámetro -0 y el parámetro -sV. La descripción de cada uno de estos parámetros se indica a continuación

- Nmap -O analiza los puertos y trata de detectar la versión del sistema operativo.
- Nmap -sV analiza los puertos abiertos y determina los servicios y la versiones que se están ejecutando.

El resultado de realizar un nmap -O -sV al sistema principal se muestra a continuación

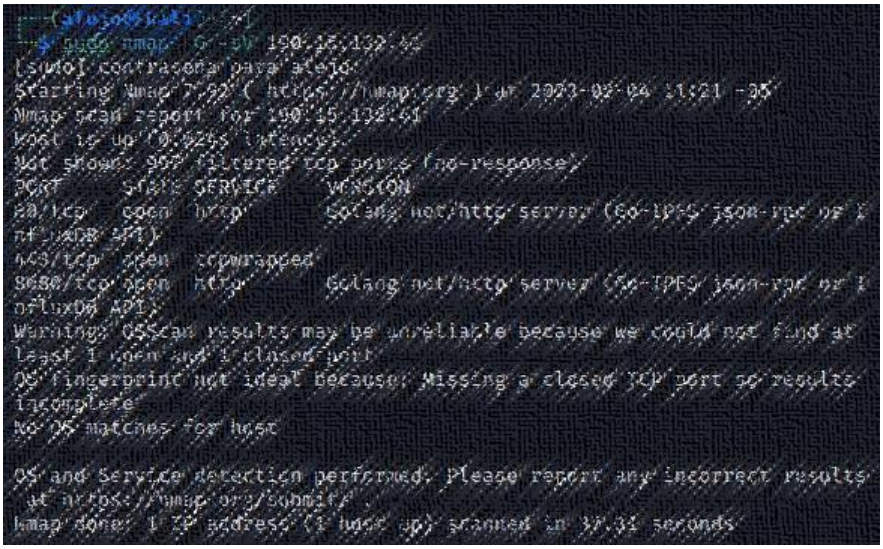


Figura 2: Resultado del análisis de puertos con Nmap sobre el servidor principal. Fuente: Propia

Los resultados que se pueden identificar al realizar el nmap en el servidor principal indican que existe la presencia de 3 puertos abiertos con sus respectivos servicios y versiones

El detalle de los hallazgos se indica en la siguiente tabla.

Tabla 20: Resumen de puertos, servicios y versiones de aplicaciones en puertos abiertos

Puerto	Estado	Servicio	Versión
80/tcp	abierto	http	Golang net/http server (Go-IPFS json-rpc or InfluxDB API
443/tcp	abierto	tcpwrapped	Fort Client VPN
8080/tcp	abierto	http	Golang net/http server (Go-IPFS json-rpc or InfluxDB API

En los hallazgos encontrados con la herramienta de seguridad y pentesting Nmap se especifican algunos puertos abiertos con su respectivo servicio y versión. Esta

información se encuentra expuesta y representa una vulnerabilidad. Los atacantes pueden aprovecharse de estos datos para encontrar recursos de explotación.

En este sentido y aprovechando los datos entregados por esta herramienta se puede consultar en las bases de datos de vulnerabilidades conocidas con el afán de encontrar debilidades de seguridad en los servicios y su respectiva versión.

Otra de las herramientas que se utilizan para el análisis de aplicaciones web y de escritorio se trata de **Nessus** con la que se puede realizar un escaneo completo de vulnerabilidades. Para disponer de este utilitario se debe descargar y instalar la versión gratuita de este software que permite un máximo de 15 destinatarios disponibles para realizar.

El análisis de vulnerabilidades de seguridad de la información se realizó al sistema de académico Fénix instalado en el servidor duplicado para no interferir en las operaciones y buen funcionamiento del sistema de producción.

Algunos de los resultados que se obtuvieron del análisis con Nessus se pueden observar en la siguiente figura.

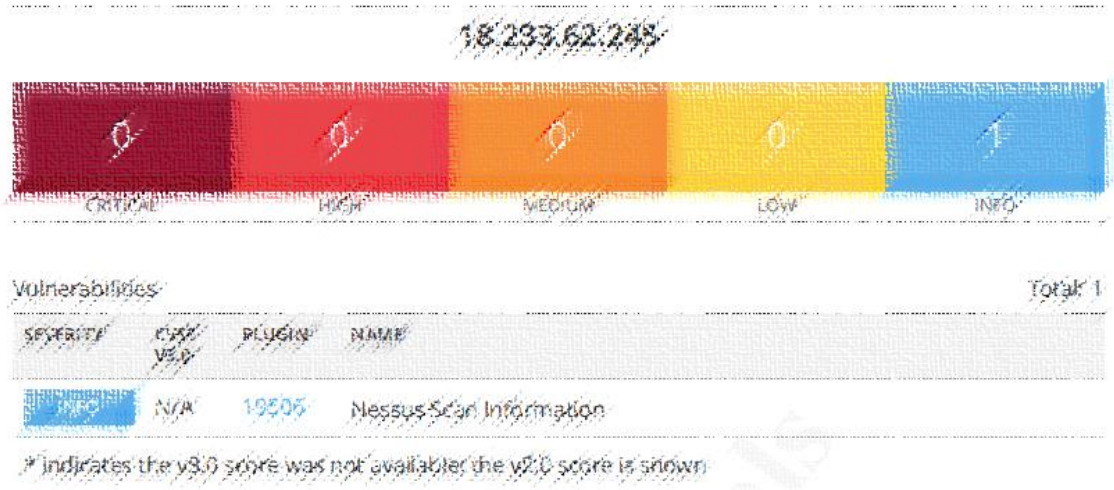


Figura 3: Resumen de hallazgos identificados con la herramienta de análisis Nessus. Fuente: Informa de resultados de la herramienta Nessus

Como se puede observar la herramienta de análisis de vulnerabilidades Nessus no pudo encontrar ninguna vulnerabilidad en el sistema Fénix instalado en el servidor duplicado. Estos resultados se deben a que el servidor duplicado se encuentra en un recurso virtual de Amazon Web Services (AWS).

3.4.3.3 Análisis de las vulnerabilidades de los usuarios

Uno de los análisis de vulnerabilidades más enfático es el realizado al personal que usa el sistema académico Fénix. Las personas que utilizan este software son docentes y personal administrativo del Instituto Superior. En muy oportuno destacar que este es

uno de los análisis más importantes a considerar y se dice que por lo general el eslabón más débil de seguridad son los recursos humanos de una organización.

Para llevar a cabo este estudio que tiene mucha relación con la ingeniería social, se ha contemplado actuar en varios frentes para poder evidenciar los hallazgos. Las técnicas utilizadas para este análisis se enumeran a continuación.

Tabla 21: Técnicas de ingeniería social a utilizar en los usuarios del sistema Fénix.

Técnicas de ingenierías social	
Interacción humana	• Visitas personales • Mensajería instantánea
Ciberataques	• Phishing

Visitas personales

Esta actividad se desarrolló con la ayuda de un grupo del personal que trabaja en el Instituto Superior donde se realizaron visitas para constatar que sus escritorios se encontraban limpios, es decir, sin la presencia de documentos confidenciales y reservados para exclusivo uso del personal.

En este estudio se visitaron 5 departamentos del Instituto y se obtuvieron los siguientes resultados

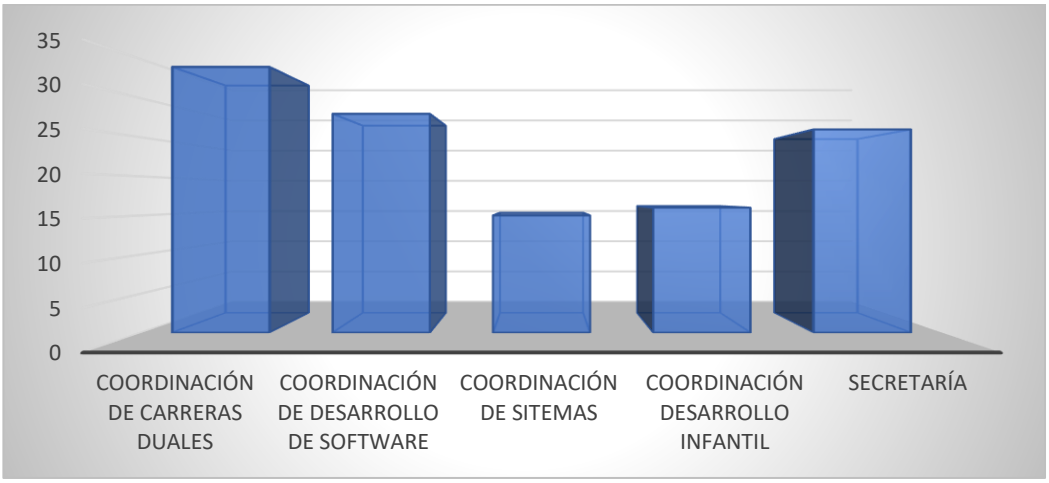


Figura 4: Cantidad de documentos por coordinación encontrados sobre los escritorios de los usuarios. Fuente: Propia

En el gráfico se puede evidenciar que se encontraron en las visitas realizadas un buen número de documentos al alcance de cualquier persona que se encuentre cerca de los escritorios. Esto representa ya una debilidad considerable de seguridad donde sin el más mínimo esfuerzo cualquier persona puede sustraer esta información.

A continuación, se muestra otro gráfico en donde se especifica el tipo y número de documentos que se encontraron en cada una de las dependencias al momento de realizar las visitas.

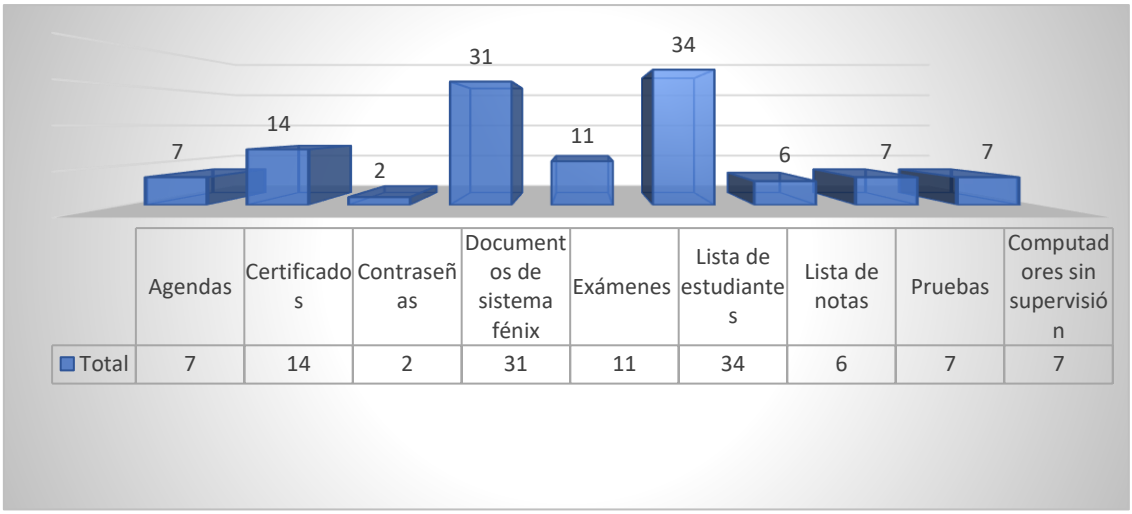


Figura 5: Detalle del tipo y cantidad de documentos encontrados sobre los escritorios de los usuarios. Fuente: Propia

Definitivamente que los lugares de trabajo del personal que trabaja en esta institución necesitan un orden y una mejor organización para guardar información confidencial y sensible. En este sentido, se puede observar documentos de estudiantes, pruebas, computadores encendidos sin bloqueo por contraseña y otros aspectos a considerar como debilidades en cuanto a la seguridad de la información.

Para poder identificar de mejor manera otras vulnerabilidades con relación a los usuarios del sistema académico Fénix se llevará a cabo en el siguiente apartado un ataque phishing al personal.

3.4.4 Escenario de Explotación

Para evidenciar las inseguridades del sistema académico Fénix se ha contemplado realizar dos explotaciones del aplicativo. En este caso se realizará un ataque mediante una vulnerabilidad de código encontrada y otro ataque mediante una vulnerabilidad del sistema.

3.4.4.1 Explotación de una vulnerabilidad de código

En el código fuente del sistema Fénix se encuentran algunas vulnerabilidades que se relacionan con la mala ejecución de métodos, uso deficiente de funciones y otras anomalías y debilidades de seguridad.

Por ejemplo, en la función de ingreso rápido "ingresoVeloz(String c)" en la clase "XXXXXXXXXX" tiene como objetivo reducir el tiempo de ingreso solo para tres usuarios que se encuentra escritos en texto claro en el código de la clase, esta función ayuda a ingresar al sistema con solo digitar 2 caracteres.

Esta vulnerabilidad puede ser descubierta con herramientas como jadx, SonarQube o java-decompiler para ser aprovechada por atacantes y realizar una suplantación de identidad directa.

Esta vulnerabilidad de clase “XXXXXXXXX”, contiene un usuario y contraseña escrita directamente en el código para ser aprovechada.

En la siguiente figura se puede apreciar parte del código que contiene las líneas de programación vulnerable con el usuario y contraseña en texto plano.

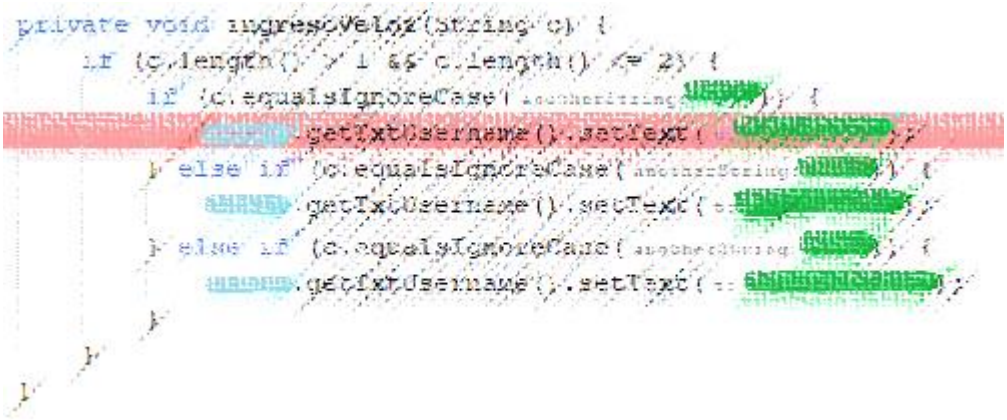


Figura 6: Porción de código fuente del sistema Fénix en donde se encuentra una vulnerabilidad expuesta. Fuente: Propia.

Para verificar que esta vulnerabilidad de seguridad de la información es una amenaza se digita los caracteres “XXX.”, en el campo usuario del ingreso al sistema académico con lo que este se auto completa en los campos usuario y contraseña.

Figura 7: Ingreso al sistema mediante la vulnerabilidad de código fuente encontrada. Fuente: Propia

En la siguiente ventana se escoge el tipo de usuario DEV que es el que posee todos los privilegios siendo este el usuario administrador.

Figura 8: Ingreso al sistema Fénix como usuario administrador mediante la vulnerabilidad encontrada. Fuente: Propia.

Luego de estos dos pasos se tiene acceso total al sistema académico Fénix y se puede acceder a todos los menús y consultar por todas las bases de datos que se desee.

3.4.4.2 Explotación de una vulnerabilidad del sistema

Para poder encontrar una vulnerabilidad del sistema es conveniente analizar los servicios que se encuentran habilitados en los puertos abiertos. En este caso el puerto que podemos analizar es el siguiente.

- Puerto 80/tcp http Golang net/http server (Go-IPFS json-rpc - InfluxDB API)

En este puerto se encuentra el servicio InfluxDB ejecutándose dentro del servidor http. Este resultado recolectado por Nmap brinda un dato relevante para poder buscar alguna debilidad de seguridad relacionada a este servicio.

InfluxDB es una base de datos de series temporales diseñada para el almacenamiento rápido y de alta disponibilidad, la misma pertenece al programa Traefik que se encuentras dentro de la plataforma de programación de Fénix. Traefik es un proxy inverso y balanceador de carga, que se integra nativamente con Docker así como con otras tecnologías de cluster que permite conectar URLs con servicios.

En una consulta web se encontraron varios sitios que ofrecen información de como vulnerar el sistema a partir de InfluxDB. Esta aplicación se trata de una base de datos de tipo temporal y se señala que esta aplicación es vulnerable en algunas versiones.

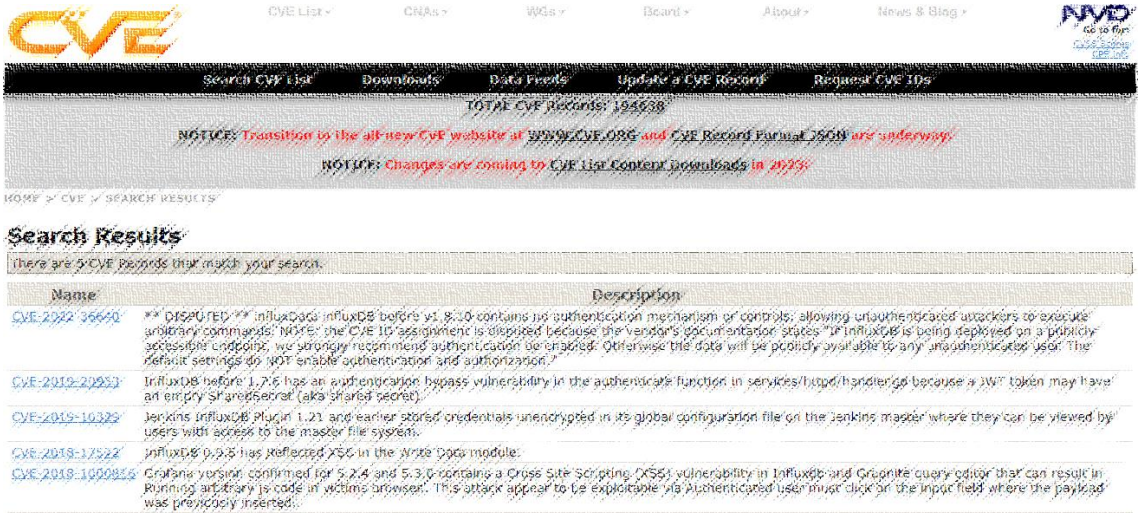


Figura 9: Vulnerabilidad bien conocida identificada en el sitio web oficial de CVE. Fuente: CVE.

La figura anterior indica que InfluxDB es susceptible a ataques reportados en los años 2018, 2019 y 2022.

En otro sitio web consultado se encuentra un recurso para poder explotar InfluxDB. En la siguiente imagen se muestra este script disponible de forma pública.

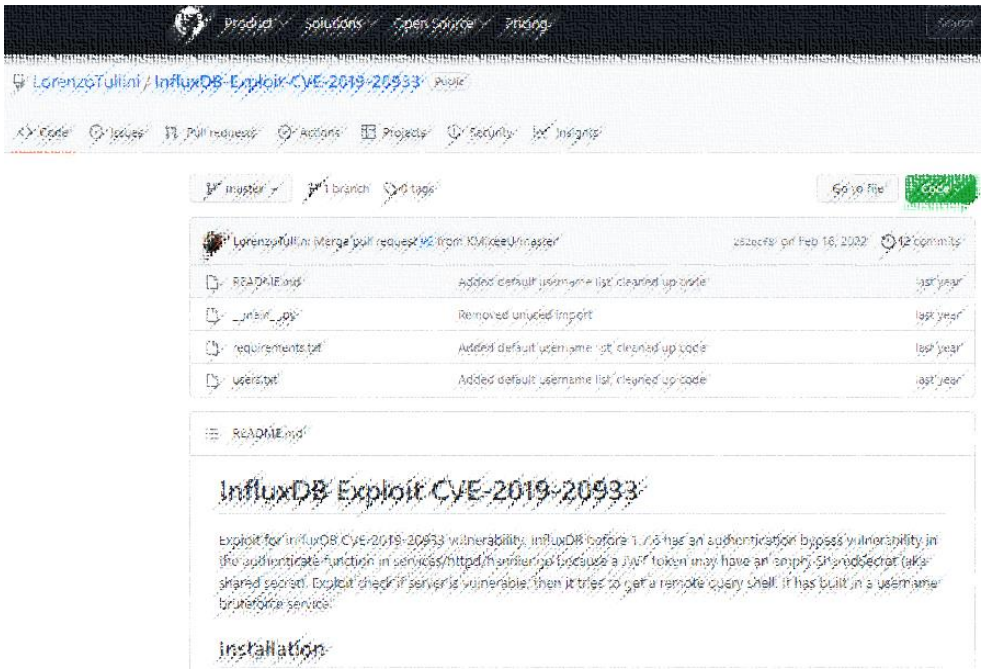


Figura 10: Repositorio de descargar del exploit InfluxDB. Fuente: Github

Con esta evidencia se puede constatar que el sistema académico Fénix es vulnerable a través de la base de datos temporal InfluxDB. La explotación de este recurso no se va a llevar a cabo por lo que al ejecutar cualquier exploit se corre el riesgo de interrumpir el buen funcionamiento del servidor principal y se podría además tener problemas legales e institucionales.

Esta vulnerabilidad según NIST tiene una ponderación de 9.8/10 catalogada como critica.

3.4.4.3 Explotación de vulnerabilidad del usuario

Phishing al personal

Como se escogió un ataque de phishing básico, se desarrollaron tres etapas para cumplir con la meta de recibir los usuarios y contraseñas del sistema fénix. En este sentido, se limitó él envió de 15 mensajes de WhatsApp y 20 correos. Se estableció un horario para el ataque y se envió el contenido a personas al azar que laboran en el Instituto. Entre los destinatarios se encuentran también 4 docentes de la a área de tecnología con el fin de evaluar la reacción de los mismos.

Para llevar a cabo esta actividad se estableció un mensaje phishing, en donde se le solicita al usuario mediante mensaje de WhatsApp ingresar a un sitio web para llenar sus datos de usuario y contraseña.

Figura 11: Mensaje de phishing enviado a los usuarios del sistema académico Fénix. Fuente: Propia.

En la figura se puede observar el texto del mensaje de phishing escrito desde la plataforma de WhatsApp.

Por otro lado, se envía este el mismo ataque de phishing mediante correo electrónico al personal con el afán de capturar alguna víctima y obtener sus credenciales. El correo que se redactó se pude observar en la siguiente imagen.

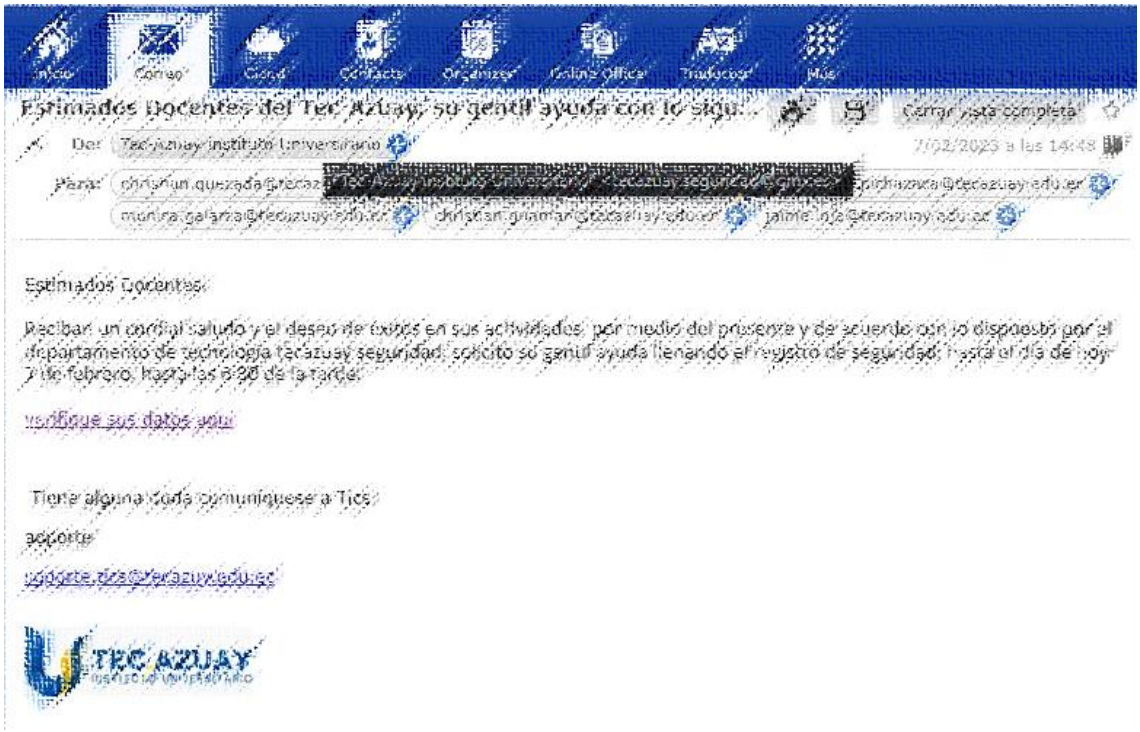


Figura 12: Correo de phishing enviado a los usuarios del sistema académico Fénix. Fuente: Propia

Tanto el mensaje de WhatsApp como el correo contienen un enlace que redirecciona a una página de encuestas en donde se solicita a la víctima llenar sus datos confidenciales de usuario y contraseña.
En la siguiente imagen se pude ver el modelo de encuesta enviada al personal en donde se solicita los datos de usuario, contraseña antigua y contraseña nueva.

El enlace de la encuesta es el siguiente: https://www.onlineencuesta.com/s/v4s3inw

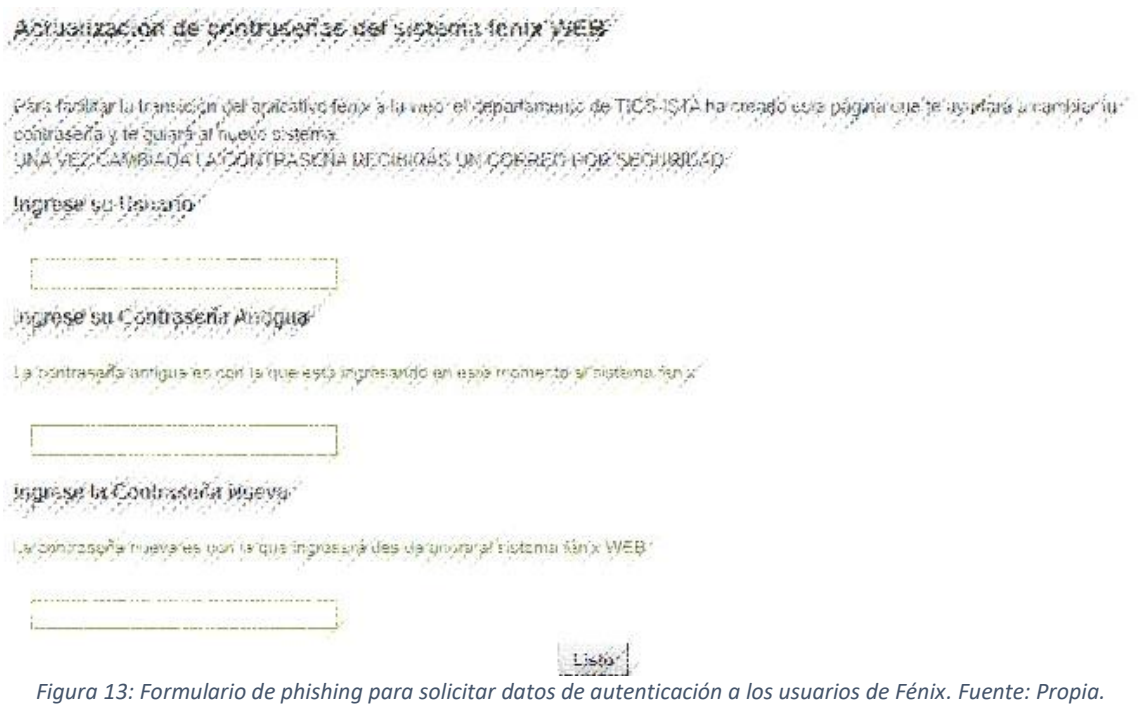


Figura 13: Formulario de phishing para solicitar datos de autenticación a los usuarios de Fénix. Fuente: Propia.

Se decide utilizar una encuesta, debido a que esta palabra no es detectada por los FIREWALLS o IDS de los correos. El ataque empezó a las 2:30 de la tarde, hora en la cual se encuentran en promedio unos 45 docentes en las instalaciones. Pará propiciar el ataque, se enviaron 19 correos y 15 mensajes de texto vía WhatsApp. No se pudo enviar el correo a más docentes por lo que los FIREWALLS o IDS de los correos no lo permitió.

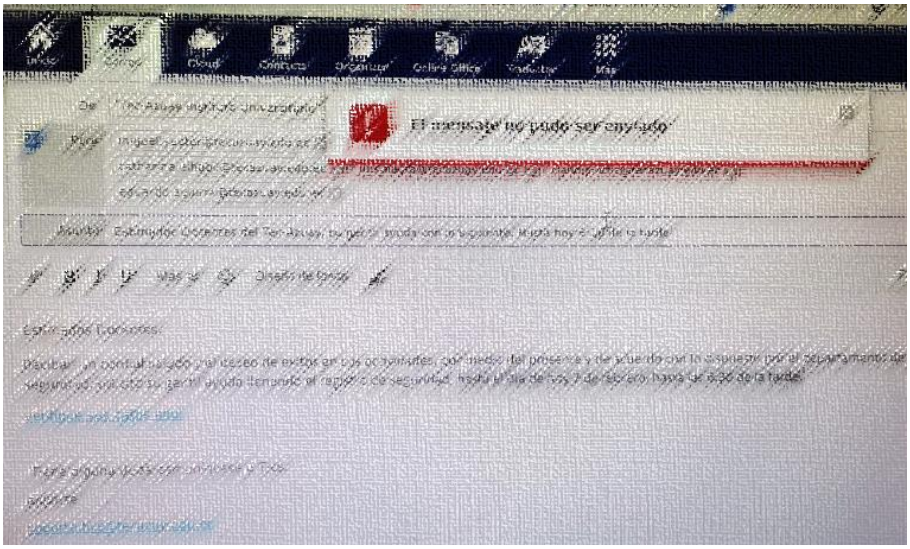


Figura 14: Bloqueo de la cuenta de phishing al tratar de enviar este correo fraudulento a más usuarios. Fuente: Propia.

Así también, WhatsApp bloqueo la cuenta al detectar el envío del mensaje a 15 usuarios.

Figura 15: Bloqueo de la cuenta de Whatsapp por el envío de mensajes phishing. Fuente: Propia.

Luego del envío del mensaje y correo phishing se procede a verificar los datos obtenidos del ataque. En la siguiente figura se puede observar el detalle de los resultados.

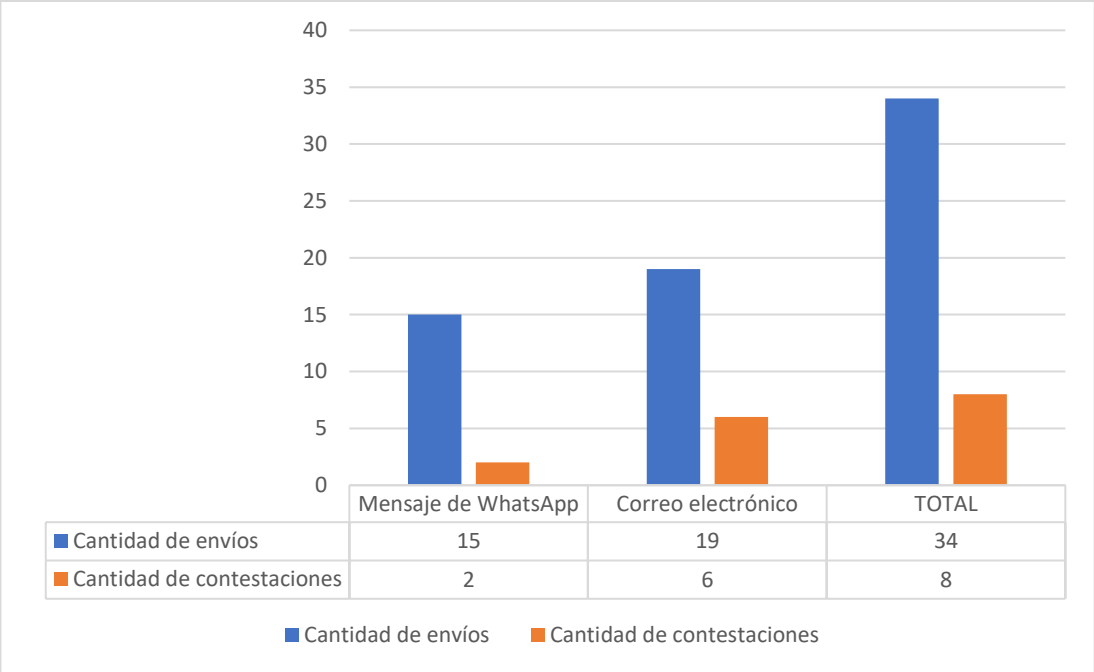


Figura 16: Resultados del ataque de phishing a los usuarios del sistema académico Fénix. Fuente: Propia.

Cabe recalcar que el total de víctimas que entregaron sus datos confidenciales constituyen el 23.5% de la muestra del personal que fue atacado.

Una de las novedades que se suscitaron en esta actividad fue un aviso comunicado de parte del departamento de TICs del Instituto en donde se pedía al personal no ingresar a la encuesta y no entregar sus datos personales. Este aviso fue enviado como reacción a evento del ataque de phishing. Este mensaje hacia todo el personal se puede evidenciar en la siguiente imagen.

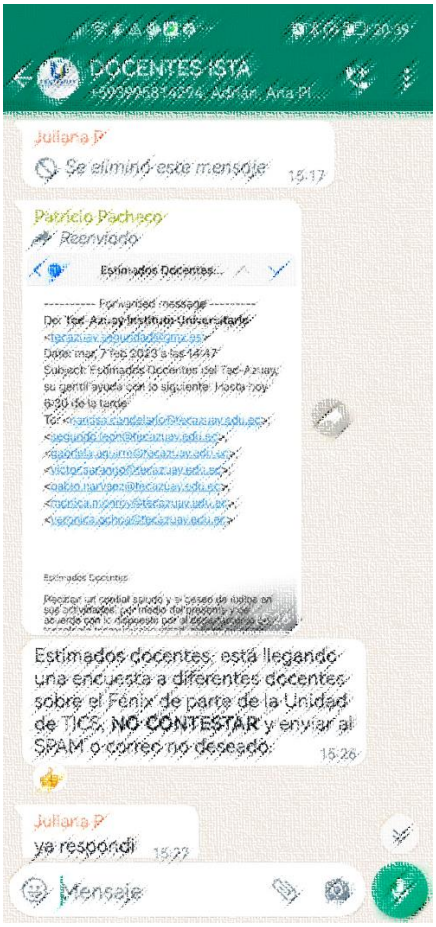


Figura 17: Mensaje de aviso del departamento de TIC indicando la identificación del ataque phishing. Fuente: Propia.

3.4.5 Post – explotación

3.4.5.1 Mitigación de la vulnerabilidad de código

Para poder sanear esta vulnerabilidad se deberá borrar la línea de código que llama a la función "ingresoVeloz(txt);" en la función "InitEventos()" para evitar el ingreso. El código después de estas modificaciones quedaría tal como se indica en la siguiente figura.

```
private void InitEventos() {
    vista.getBtnIngresar().addActionListener(e -> login());
    Efecto1 btnHover = new Efecto1(vista.getBtnIngresar(), vista.
    vista.getTxtPassword().addKeyListener(new eventoTexto());
    vista.getTxtUsername().addKeyListener(new eventoTexto());

    vista.getTxtUsername().addKeyListener(new KeyAdapter() {
        @Override
        public void keyReleased(KeyEvent e) {
            String txt = vista.getTxtUsername().getText().trim();
            if (txt.length() <= 2) {
                vista.getTxtPassword().setText("Libre_OS");
            }
```

Figura 18: Remediación de la vulnerabilidad de código fuente. Fuente: Propia.

Para finalizar esta mitigación se debe también borrar la “funcion private void ingresoVeloz(String c)” de la Clase LoguinCTR.

Figura 19: Intento fallido del ingreso al sistema Fénix mediante la vulnerabilidad de código subsanada. Fuente: Propia.

Como se puede observar en la figura anterior al ingresar los caracteres “M.” ya no se autocompleta el usuario y el password en el formulario.

3.4.5.2 Mitigación de la vulnerabilidad de sistema

La vulnerabilidad del sistema InfluxDB encontrado en el apartado anterior referente al escenario de explotación es posible mitigarla. En los sitios web oficiales de NIST y CVE se recomienda realizar un proceso de autenticación robusto y si es posible con doble factor. Esta aplicación se encuentra por defecto configurada sin permisos de autenticación lo que conlleva un riesgo serio.

Otra de las medidas de mitigación es actualizar la versión de InfluxDB o cambiar a otro gestor de base de datos más actual que contenga las ultimas actualizaciones de parches de seguridad conocidas.

Por último, para contrarrestar esta amenaza se podría fortalecer el escenario de registro de eventos en los que se pueda controlar los parámetros de ingreso a la base de datos y un posible registro de cambios.

3.4.5.3 Mitigación de vulnerabilidades de usuarios

Para poder encontrar las vulnerabilidades relacionadas a los usuarios se llevó a cabo un ataque de phishing como se detalló anteriormente. Como parte de la mitigación de este suceso el personal de TIC del Instituto dio un aviso por Whatsapp indicando que no llenen el formulario del ataque. Esta acción de tipo reactiva no fue tan efectiva y al paso de algunos minutos dos personas más respondieron la encuesta.

La mitigación de vulnerabilidades relacionadas a los usuarios del sistema Fénix se logra con la concientización y educación de los usuarios en temas de seguridad de la información. En este sentido la implementación de las políticas, procedimientos, buenas prácticas y campañas son algunas de las herramientas que se pueden utilizar para fortalecer el eslabón más débil de seguridad que por lo general son personas que trabajan en la Institución.

En el siguiente capítulo referente al desarrollo de marcos de políticas y recomendaciones se profundizará los procesos que se tienen que seguir para solventar las inseguridades de los usuarios del sistema Fénix.

4 Marco de políticas y recomendaciones

En este apartado se propone una serie de políticas de seguridad y recomendaciones para disminuir la cantidad de vulnerabilidades que se identificaron en el capítulo anterior dentro del sistema académico Fénix. A continuación, se describen los detalles de estas buenas prácticas de seguridad de la información.

4.1 Marco de Políticas de Seguridad de la Información

En este apartado se propone la aplicación de un marco de políticas de seguridad de la información con la finalidad de fortalecer la seguridad del sistema académico Fénix del Instituto Superior. En este sentido los siguientes puntos especifican los detalles de este marco.

Marco de políticas de seguridad de la información

Para mitigar las vulnerabilidades encontradas en el sistema académico Fénix se proponen las siguientes medidas de ciberseguridad dentro de un marco de políticas tomando como referencia la norma ISO 27002:2022 que se describen a continuación:

4.1.1 Políticas de Relación laboral

Las políticas de relación laboral que se propone implementar en los usuarios del sistema Fénix son:

- El Departamento de recursos humanos deberá presentar a trabajadores, docentes y empleados del Instituto la suscripción de un acuerdo de confidencialidad, no divulgación de la información y uso adecuado de los sistemas de información. Control de Referencia 6.6 Acuerdo de Confidencialidad o no divulgación.

- Los trabajadores que se desvinculen de la Institución deberán participar en un proceso bien establecido en donde se lleve a cabo la devolución de activos de información, el cierre y bloqueo de todos sus accesos y el borrado de datos de información institucional. Control de referencia 5.11 Devolución de activos de seguridad.

4.1.2 Políticas de Gestión de Activos de Seguridad

Las políticas también buscan resguardar la integridad, disponibilidad y autenticidad de los activos de seguridad de la información. En este caso se deberán implementar los siguientes lineamientos:

- El departamento de TIC en trabajo conjunto con las coordinaciones y jefaturas del Instituto deberán mantener un inventario actualizado de los activos de información y su respectivo responsable. Control de referencia 5.9 Inventario de información y otros activos asociados.

- El responsable del activo de seguridad de la información deberá asegurar su buen uso, custodia y protección. Control de referencia 5.11 Uso aceptable de la información y otros activos asociados.

4.1.3 Políticas para la clasificación y etiquetado de documentos

Los documentos digitales y físicos deberán ser clasificados y etiquetados según los siguientes tipos: Documentación pública, documentación interna y documentación confidencial.

- Documentación publica: Información disponible para la colectividad en general.
- Documentación interna: Información usada y reconocida por usuarios internos.
- Documentación confidencial: Información que está avalada por un autor o propietario y que debe ser autorizada para su publicación.

Control de referencia 5.12 Clasificación de la información y 5.13 Etiquetado de la información.

4.1.4 Políticas de protección antimalware

Las políticas también buscan proteger a los activos se seguridad de la información de infecciones de software malicioso. Las políticas para este apartado son:

- La Unidad de TIC deberá implementar soluciones antimalware en todos los equipos informáticos del Instituto.
- La Unidad de TIC deberá realizar análisis periódicos de software malicioso con un sistema antimalware.
- La herramienta antimalware deberán ser capaz de prevenir y detectar software malicioso.
- La herramienta antimalware deberá ser capaz de mantener actualizados sus registros y componentes.

Control de referencia 8.7 Protección contra el malware.

4.1.5 Políticas sobre el uso de internet, correos electrónicos y mensajería.

Las políticas que aplican al uso del internet, correo electrónico y mensajería son:

- El uso del servicio de internet se limitará a consultas de tipo académicas, investigativas, operativas y otras relacionadas a la educación.
- Las cuentas de correo institucionales serán exclusivamente utilizadas para uso institucional.
- No se deberá responder o reenviar correos catalogados como spam, cadenas de mensajes y correos de remitentes desconocidos y se debe proceder a eliminarlos de forma definitiva.
- La documentación interna y la documentación confidencial enviada, recibida o almacenada deberá ser gestionada solamente a través de cuentas institucionales.

Control de referencia 5.14 Transferencia de información y 8.21 Seguridad de los servicios de red.

4.1.6 Política de gestión de riesgos

Los activos de la seguridad de la información críticos deberán ser incluidos en un estudio de análisis de gestión de riesgos con metodología correspondiente en donde se identifiquen las amenazas, impacto y tratamiento de mitigación sugeridos.

Control de referencia 5.7 Inteligencia sobre amenazas.

4.1.7 Políticas de concientización de usuarios

Ejecutar campañas de información y capacitación en donde se promuevan las buenas prácticas de seguridad de la información con el afán de crear conciencia sobre la protección y preservación de la información Institucional. Estas campañas deberán estar enfocadas a socializar las Políticas de Seguridad de la Información.

Control de referencia 6.3 Sensibilización, educación y formación en materia de seguridad de la información.

4.1.8 Políticas de controles de seguridad

La Unidad de TIC deberá implementar configuraciones, reglas y controles de seguridad en firewall, proxy, IPSs, IDs y demás herramientas de seguridad para garantizar la protección de datos que ingresen a la red de comunicación interna de la Institución.

Control de referencia 8.20 Seguridad de las redes y 8.21 Seguridad de los servicios de red.

4.1.9 Política para el cifrado de la información

La unidad de TIC deberá implementar el cifrado de la información en bases de datos y discos de almacenamiento incluyendo contraseñas de acceso.

El cifrado también se debe incluir en usuarios y contraseñas de administrador o superusuario resguardando esta información en lugares estratégicos y seguros de la infraestructura informática

Control de referencia 8.24 Uso de la criptografía.

4.1.10 Política para la gestión de registros de eventos

La unidad de TIC deberá implementar un sistema de registro de eventos o pistas de auditoría para el acceso o modificaciones de la información confidencial o reservada en las aplicaciones de información.

Estos eventos realizados por el usuario deberán corresponder a:

- Hora y fecha de ultimo acceso o intento de acceso.
- Dirección IP y otros parámetros relacionados de la máquina que se conecta.
- Cambios de estado de usuario (activo, inactivo, bloqueo)
- Número de intentos de acceso fallidos y exitosos.
- Fecha y hora de cambio de contraseña

Control de referencia 6.8 Informes de eventos de seguridad de la información y 5.25 Evaluación y decisión sobre eventos de seguridad de la información

4.1.11 Política para la autenticación

La unidad de TIC deberá implementar un sistema centralizado de autenticación y un sistema de doble factor de autenticación para aplicaciones críticas.

Control de referencia 5.17 Información de autentificación.

4.1.12 Política de contraseñas

Las políticas para gestionar el uso y creación de contraseñas se definen a continuación:

- Deberán disponer de una longitud de 8 caracteres.
- Las contraseñas deberán contener al menos dos de los siguientes grupos de caracteres: mayúsculas, minúsculas, numéricos, especiales.
- Se prohíbe usar nombres, fechas de nacimiento, domicilios o palabras de diccionario o comunes relacionadas con su identificador de usuario.
- Los sistemas informáticos de la Institución deberán obligar al usuario a cambiar su contraseña en su primer ingreso.

- Luego de 5 intentos fallidos de inicio de sesión se realizará el bloqueo de la cuenta de usuario.
- Se debe especificar cambios de contraseñas de usuario mínimo cada 6 meses.

Control de referencia 5.17 Información de autentificación.

4.1.13 Políticas de respaldos de seguridad

El departamento de TIC deberá contar con procedimientos aprobados para realizar copias de seguridad de la información de bases de datos, servidores, aplicaciones, código fuente, entre otros, considerando aspectos como: frecuencia, tiempo de retención, verificación, almacenamiento en una ubicación remota.

Control de referencia 8.13 Información de respaldo

4.1.14 Política de la seguridad física en las instalaciones

Las instalaciones de procesamiento de información como: centros de datos, cuartos de comunicaciones y las instalaciones del departamento de TIC, deberán contar con sistemas que garanticen el registro y control del acceso físico, con sistemas biométricos, lectores de tarjetas magnéticas o identificación por radiofrecuencia. Este sistema de control de acceso deberá mantener el histórico de accesos a estas áreas de procesamiento de información.

Control de referencia 7.1Perímetro de seguridad física y 7.2 Entrada física

La tabla resumen de las políticas de seguridad asociados al control de seguridad del sistema Fénix se pueden observar en el Anexo F.

4.2 Recomendaciones de seguridad

Luego de la explicación del marco de políticas sugerido para el sistema académico Fénix, se presenta también una serie de recomendaciones basadas en el marco de recomendaciones de ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST). A continuación, se describen las siguientes recomendaciones de NIST 800 53 Framework versión 1.1 basadas en estas cinco áreas: identificación, protección, detección, respuesta y recuperación.

Fase de Identificación

- Realizar una lista de registro de los activos de información para posteriormente realizar un estudio de análisis de riesgos.
- Elaborar y compartir las Políticas de Seguridad de la Información Institucional

Fase de Protección

- Controlar el acceso a la red interna, computadoras y otros dispositivos.
- Usar aplicativos de seguridad para salvaguardar los datos.
- Clasificar y codificar los documentos críticos.
- Hacer copias de seguridad de los datos con la periodicidad adecuada.
- Actualizar los programas de seguridad con regularidad de ser posible de forma automática.
- Implementar procedimientos formales para la eliminación segura de documentos digitales y equipos en desuso.
- Capacitar en temas de ciberseguridad a todas las personas que laboren en la Institución que usen sus computadoras, dispositivos y redes.

Fase de Detección

- Monitorear la seguridad de la red para detectar y controlar el acceso no autorizado a equipos, dispositivos (soportes de almacenamiento de datos de tipo USB) y software.
- Revisar la red para identificar y controlar si detecta usuarios o conexiones no autorizados.
- Investigar cualquier actividad sospechosa en la red.

Fase de Respuesta

- Implementar un plan para notificar los activos de seguridad de la información críticos.
- Implementar un plan de continuidad de negocio.
- Implementar un plan para reportar ataques de ciberseguridad.
- Implementar un plan para investigar y contener un ataque.
- Implementar un plan para la actualización de las políticas de seguridad de la información tomando como referencia las lecciones aprendidas.
- Implementar un plan de preparación ante riesgos de carácter natural.

Fase de Recuperación

- Después de un ataque reparar y restaurar los equipos y las partes de su red que resultaron afectados.
- Después de un ataque mantenga informados a sus trabajadores sobre las actividades de respuesta y recuperación.

5 Resultados y discusión

Los resultados y su discusión se detallas a continuación.

5.1 Resultados

El análisis de vulnerabilidades del sistema académico Fénix del Instituto Superior se llevó a cabo de forma satisfactoria de acuerdo a lo planificado y cumpliendo con los tiempos establecidos obteniendo los resultados de las diversas pruebas realizadas. La metodología aplicada para el desarrollo de este análisis se fundamentó en el Estándar de Ejecución de Pruebas de Penetración (PTES) que incluye 7 secciones claramente identificadas y cumplidas a cabalidad.

Mediante indagación bibliográfica física y digital se completó efectivamente el análisis del estado del arte relacionado con trabajos actuales relacionados con el análisis de vulnerabilidades aplicadas en instituciones de educación superior. Este estudio se obtuvo a partir de artículos internacionales, nacionales y locales relacionados a las vulnerabilidades de ciberseguridad.

La ejecución del hackeo ético para el descubrimiento de las vulnerabilidades del sistema académico Fénix se efectuó siguiendo la planificación, en donde la aplicación del Estándar de Ejecución de Pruebas de Penetración (PTES) fue de mucha ayuda y organización para efectuar los análisis. Considerando sus 7 secciones y el uso de herramientas especializadas se pudo obtener resultados precisos en cuanto al número de vulnerabilidades, su tipo y criticidad.

Los resultados que se encontraron en el proceso del hackeo ético se especifican en la siguiente tabla:

Tabla 22: Resumen de resultados encontrados en el proceso de hackeo ético.

Análisis de vulnerabilidades (Hackeo Ético)			
Etapa	**Tipo de análisis**	**Herramienta / Recurso**	**Resultados**

Análisis de vulnerabilidades	Código fuente	SonarQube	Se encontraron 85 anomalías de código, 4 vulnerabilidades, 6200 caracteres de código sucio, 7 puntos de acceso, 4357 líneas duplicadas de código, 266 bloques duplicados y 86 archivos duplicados.
		OWASP Dependency Check	Se encontraron 19 vulnerabilidades con incidencia crítica, 11 con nivel alto y 10 con vulnerabilidad nivel medio
	Sistema Fénix	Nmap	Se encontraron 3 puertos abiertos: • 80/tcp/ http/ Golang net/http server (Go-IPFS json-rpc or InfluxDB API • 443/tcp/ cpwrapped/ Forti Client VPN • 8080/tcp/ http Golang net/http server (Go-IPFS json-rpc or InfluxDB API
		NESSUS	No se encontraron vulnerabilidades
	Gestión de Usuarios	Visitas	En las visitas a los puestos de trabajo de los empleados se encontró a la mano: 7 agendas, 14 certificados, 2 contraseñas, 31 documentos del sistema Fénix, 11 exámenes, 34 listas de estudiantes, 6 listas de notas, 7 evaluaciones y 7 computadoras prendidas sin bloquear.
Explotación de vulnerabilidades	Código fuente	XXXXXX	La vulnerabilidad de clase “XXXXXXXX”, contiene un usuario y contraseña escrita directamente en el código para ser aprovechada
	Sistema Fénix	InfXXXX	Se identifico que en el puerto 80 se encuentra en ejecución la aplicación InfXXXXX sin actualizar. Existe varios exploits para poder atacar y escalar privilegios.
	Gestión de Usuarios	Phishing	Se realizó un ataque phishing donde el total de víctimas que entregaron sus datos confidenciales constituyen el 23.5% de la muestra del personal que fue atacado.
Post-explotación de vulnerabilidades	Código fuente	Borrado de funciones	Se procede a eliminar la función XXXXXX junto con los datos e usuario y contraseña escritas en el

			código para mitigar esta vulnerabilidad.
	Sistema Fénix	Doble factor de autenticación	Se propone actualizar la aplicación InfXXXXX a su versión más actual o integrar un sistema de doble factor de autenticación.
	Gestión de Usuarios	Concientización y educación	Implementación de las políticas, procedimientos, buenas prácticas y campañas de concientización para mitigar las vulnerabilidades de los usuarios.

Al concluir los análisis de vulnerabilidades e identificar cada una de estas, permite definir una propuesta de políticas de seguridad de la información y recomendaciones basados en la Normas 27002:2022 y NIST 800 53 Framework versión 1.1, para mitigar o minimizar las vulnerabilidades presentes en el sistema académico Fénix y su infraestructura tecnológica y de personal relacionado. En este proceso se detallan reglas y controles de seguridad a nivel físico y lógico de los activos de información, así como también políticas relacionadas a la seguridad de los usuarios del sistema.

5.1.1 Reportes

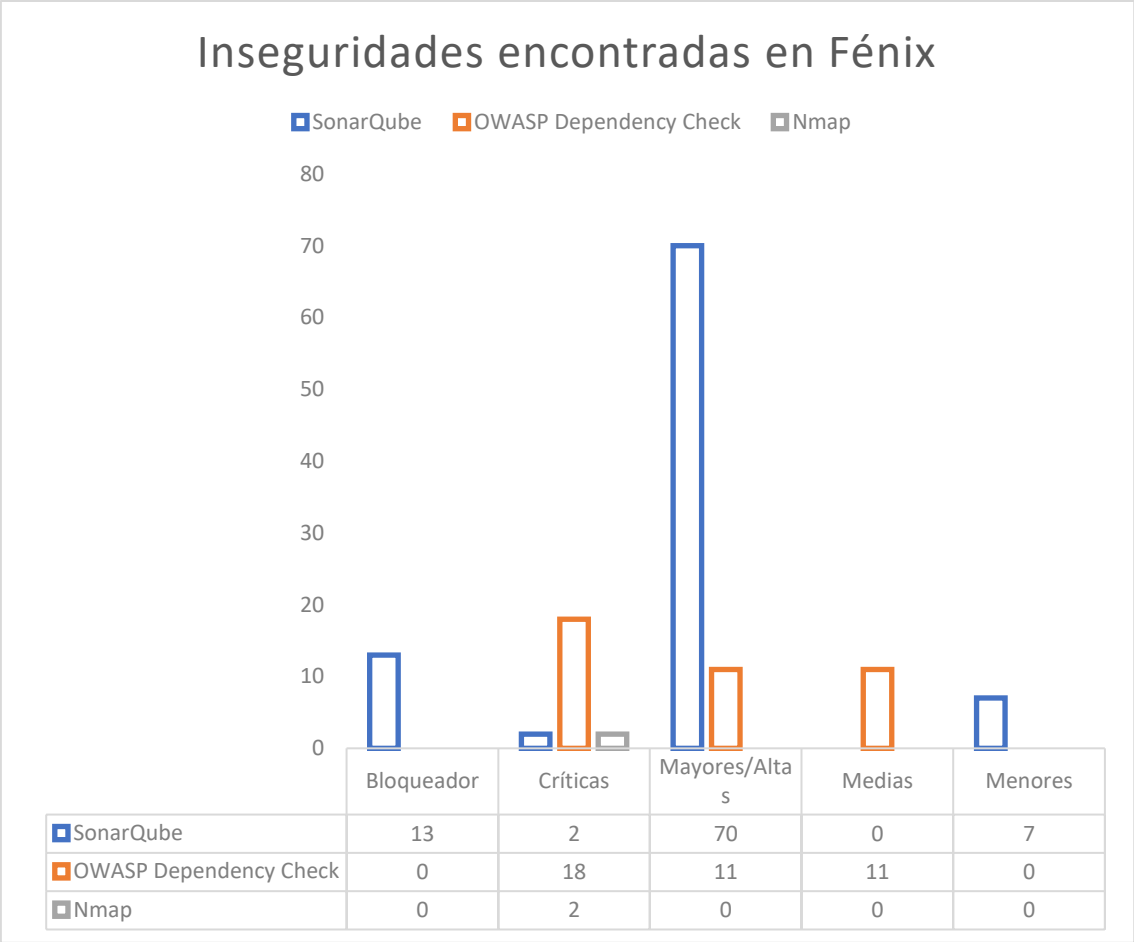
Los reportes de algunas herramientas se obtienen de forma automática después del análisis respectivo. Las herramientas de análisis de vulnerabilidades de OWASP Dependency Check entregan sus reportes de forma gratuita.

En el caso de la herramienta SonarQube no genera un reporte como tal con la versión gratuita, este documento solo es posible descargarlo si se tiene la versión de pago. Para recolectar los resultados se puede ir grabando en pdf los diferentes resultados de la aplicación web de SonarQube.

Nmap al ser una herramienta de código abierto y gratuita entrega un reporte de análisis de puertos con la integración de algunos parámetros en el comando de ejecución del análisis. En este sentido, el informe de Nmap se puede visualizar en formato de texto simple.

La herramienta Nessus entrega su reporte sin ningún costo adicional pero solo para los primeros 15 análisis. A partir del estudio 16 ya se solicita comprar la versión de pago del sistema. Cabe recalcar que Nessus se utilizó en la plataforma del servidor de respaldo por lo que no generó resultado de inseguridad.

En la siguiente tabla se puede observar el resumen de hallazgos identificados por las herramientas que realizaron el análisis en el sistema académico Fénix.



	Bloqueador	Críticas	Mayores/Altas	Medias	Menores
SonarQube	13	2	70	0	7
OWASP Dependency Check	0	18	11	11	0
Nmap	0	2	0	0	0

Figura 20: Resumen de vulnerabilidades encontradas por distintas herramientas en el sistema Fénix. Fuente: propia.

Los detalles de los hallazgos de reflejan en los reportes de cada una de estas herramientas reposan en los siguientes anexos:

- El reporte de SonarQube se encuentra en el ANEXO G.
- El reporte de OWASP Dependency Check se encuentra en el ANEXO H.
- El reporte de Nmap se encuentra en el ANEXO I.
- El reporte de Nessus se encuentra en el ANEXO J.

En conclusión, se puede indicar que se tiene un 17,32% de vulnerabilidades de nivel crítico y un 63,78% de vulnerabilidades de nivel alto lo que refleja una realidad insegura del entorno del sistema Fénix. Es recomendable actuar lo más pronto posible y mitigar estas vulnerabilidades con la tomar de accionas referentes a buenas prácticas de seguridad y la implementación de políticas de seguridad

5.1.2 Encuestas

Dentro del proceso de recolección de información necesaria para el análisis de vulnerabilidades es oportuna la realización de una encuesta dirigida al personal del Instituto. En esta ocasión se excluye a los estudiantes del Instituto debido a que no

tienen un contacto directo con el sistema académico Fénix. Los detalles de las preguntas de la encuesta se pueden revisar en el Anexo K y los resultados de las encuestas en el Anexo L.

Las encuestas fueron aplicadas a 14 funcionarios del Instituto Superior entre los cuales destacan 3 personas del área de tecnologías de la información y comunicación, 9 del área docente, 1 del área administrativa y 1 persona de investigación. El periodo de tiempo de trabajo en la institución de los encuestados es muy variado. Existen 2 personas que han trabajado menos de un año y 7 que han trabajado más de 5 años.

De igual manera, las respuestas a las preguntas de la encuesta son muy variadas donde destaca el tema de seguridad de la información que integra el sistema académica Fénix. En este punto, el 50% de los encuestados tiene una percepción pobre del sistema en cuanto recursos de seguridad que dispone.

Entre las respuestas de los encuestados acerca de las inseguridades del sistema se pueden rescatar las siguientes observaciones:

- Desconocimiento en temas de seguridad de la información.
- No exige parámetros de seguridad informática.
- Falta de recursos economicos para proveer seguridad.
- Manejo de usuario y contraseñas debil.
- Se puede acceder al sistema facilmente

5.2 Discusión

Dentro del análisis de hackeo ético se obtuvieron resultados con la ayuda de herramientas de software de última generación por lo que difiere de otros análisis llevados a cabo en otras instituciones de educación y otros escenarios. En este sentido por ejemplo la herramienta SonarQube no se ha evidenciado en otros tipos de análisis, pero resulta ser una herramienta de análisis muy versátil y robusta cuando se desea verificar las vulnerabilidades en la estructura de código.

Algunas vulnerabilidades encontradas comúnmente se relacionan con puertos de red abiertos, en este caso los resultados de análisis de vulnerabilidades muestran tres puertos abiertos que se encuentran vinculados con aplicaciones que reflejan un factor estándar de inseguridad que se relaciona con la desactualización de estos componentes.

Otro de los factores comúnmente identificados en este análisis y en otros del mismo tipo se encuentra el control y aplicación inadecuada de políticas de seguridad de la información en donde se incluyen aspectos como buenas prácticas de contraseñas de seguridad, escritorio limpio y bloqueo pantallas. Estos parámetros son comunes de encontrar en procesos de análisis de vulnerabilidades sobre todo cuando se hace referencia a los usuarios.

Otros resultados comúnmente encontrados en varios análisis hacer referencia a los ataques simulados de phishing en donde se logra medir la vulnerabilidad de los usuarios

al recibir un correo electrónico fraudulento. Es por esta razón que la educación y concientización como parte de las políticas de seguridad de la información resulta muy necesario y efectivo al momento de proteger los activos de información.

6 Conclusiones

Como conclusiones podemos anotar:

- El análisis de vulnerabilidades realizado al sistema académico Fénix del Instituto Superior se desarrolló con un alto porcentaje de componente práctico en donde se pudieron utilizar las herramientas y recursos de seguridad de la información con la finalidad de obtener y evidenciar los resultados de inseguridad altos que mantiene actualmente la aplicación de gestión académica.
- La literatura investigada con la que se construyó el estado del arte fue enfocado a métodos de análisis de vulnerabilidades realizadas en sistemas de centros de educación superior. El artículo más relevante denominado “Information System Security Analysis to Determine Server Security Vulnerability with Penetration Testing Execution Standard (PTES) Method atVWX University”, publicado en el 2021, fue tomado como referencia para la aplicación del método de análisis de vulnerabilidades del sistema académico Fénix por ser el más actualizado y eficiente.
- En la planificación y ejecución del análisis de vulnerabilidades se escogieron las herramientas de seguridad de la información específicas e idóneas para cada caso de estudio. En este sentido se utilizó para el análisis de vulnerabilidades de código fuente la herramienta SonarQube versión 9.7.1, para el análisis de dependencias y librarías se utilizó el recurso OWASP Dependency Check versión 8.0.0 y para el análisis de la aplicación como tal se utilizó Nmap versión 7.9 y Nessus versión 10.5.0.
- Las políticas de seguridad de la información propuesta, así como las recomendaciones de ciberseguridad constituyen la línea de partida para mitigar las vulnerabilidades del activo Fénix desde todos sus frentes. Estos consejos incluye controles de seguridad para los usuarios, equipos, sistema Fénix y sus bases de datos, que pueden servir para sistemas similares futuros.
- En el desarrollo del presente trabajo de titulación en donde se analizó el estado de seguridad de la información del sistema académico Fénix se evidencio la presencia de algunas vulnerabilidades informáticas enfocadas principalmente en errores de código, versiones desactualizadas de software, vulnerabilidades en las aplicaciones de cara a los puertos abiertos y debilidades de seguridad del personal que opera el sistema al no tener una cultura de ciberseguridad y protección de los activos.

7 Recomendaciones

Como recomendaciones se puede señalar lo siguiente:

- Implementar las políticas de seguridad de la información que se detallaron en el capítulo cuatro para robustecer el entorno del sistema académico, puesto que es necesario tomar acciones, colocar controles y realizar actualizaciones.
- Realizar un nuevo análisis de vulnerabilidades luego de implementar las políticas de seguridad sugeridas a fin de verificar la disminución de fallas de seguridad y debilidades encontradas en este estudio.
- Seguir las recomendaciones de seguridad de NIST contempladas en el capítulo cuatro en donde se detallan las sugerencias ha implementar para las fases de identificación, protección, detección, respuesta y recuperación.
- Capacitar a los usuarios del sistema académico en temas de seguridad de la información para concientizar la gran cantidad de amenazas de ciberseguridad que se asociación con la ingeniería social.

8 Referencias

[1] Consejo de Aseguramiento de la Calidad de la Educación Superior, «CACES Consejo de Aseguramiento de la Calidad de la Educación Superior,» 2022. [En línea]. Available: https://www.caces.gob.ec/institutos-superiores-tecnicos-y-tecnologicos-2/..

[2] M. Zúñig y D. N. Valarezo, «La Ciberseguridad y su concepción en las PYMES de Cuenca, Ecuador. Contabilidad y Auditoría,» 2021.

[3] J. G. , «Estudio de Seguridad informática en el Sistema Académico del Ministerio de Educación,» Trabajo de titulación – Universidad Técnica de Babahoyo, 2017.

[4] A. Vallejo y R. Proaño, «Análisis de vulnerabilidades en aplicativos web e infraestructura para una institución educativa privada de la ciudad de Quito,» Trabajo de titulación – Universidad Tecnológica Equinoccial, 2017.

[5] M. I. R. Castro, G. L. F. Morán, D. S. V. Navarrete, J. E. Á. Cruzatty, G. R. P. Anzúles, C. J. Á. Mero y M. A. C. Merino, «Introducción a la seguridad informática y el análisis de vulnerabilidades,» 3Ciencias, 2018.

[6] AO Kaspersky Labs, «Ciberamenaza - Mapa en tiempo real,» Kaspersky, 2021. [En línea]. Available: https://cybermap.kaspersky.com/es.

[7] J. LLerena, A. Mendez y F. Sánchez, «Analysis of the Factors that Condition the Implementation of a Backhaul Transport Network in a Wireless ISP in a Unlicensed 5 Ghz Band, in the Los Tubos Sector of the Duran Canton,,» Conf. Inf. Syst. Comput. Sci. INCISCOS, 2019.

[8] S. Acosta, «Implementación de sistema de matriculación y carnetización en la unidad educativa Pablo Picasso,» [En línea]. Available: https://dspace.ups.edu.ec/handle/123456789/16844.

[9] C. Senarak, «Port cybersecurity and threat: A structural model for prevention and policy development," Asian J. Shipp,» Logist, 2021.

[10] S. Mukdasanit y S. Kantabutra, «Attack and defense in the layered cyber-security model and treir approximation schemes,» J. Comput. Syst. Sci, 2021.

[11] H. Zhang, B. Lui y H. Wu, «Smart Grid Cyber-Physical Attack and Defense: A Review.,» IEEE Access, 2021.

[12] C. Murillo, «Desarrollo de aplicaciones web para la gestión y control académico de la escuela particular Lidia Dean de Henriquez,» [En línea]. Available: https://dspace.ups.edu.ec/handle/123456789/17146.

[13] J. Quevedo, «Investigación y prueba de cyberdelito,» 2017. [En línea]. Available: https://www.tdx.cat/bitstream/handle/10803/665611/JQG_TESIS.pdf?sequence=1&isAllowed=y.

[14] F. Reyes, W. Fuertes, C. Guzmán, E. Pérez, P. Bernal y C. Villacís, «Application of business intelligence for analyzing vulnerabilities to increase the security level in an academic CSIRT,» *Revista Facultad de Ingeniería,* vol. 27, pp. 21 - 29, 2017.

[15] D. Gondón y R. VIllamar, «Análisis de Estrategias de Gestión de Seguridad Informática con Base en la Metodología Open Source Security Testing

Methodology Manual (OSSTMM) para la Intranet de una Institución de Educación Superior,» *Revista electrónica de Computación, Informática, Biomédica,* vol. 7, nº 1, pp. 1-21, 2018.

[16] N. A. Z. J. S. M. C. M. Z. B. Jessica Johanna Morales Carrillo, «Ciberseguridad y su aplicación en las Instituciones de Educación Superior,» *Revista Ibérica de Sistemas e Tecnologias de Informacion ,* p. 448, 2019.

[17] M. Leguizamón, M. Bonilla y C. León, «Analysis of computer attacks through Honeypots in the District University Francisco José de Caldas,» *Ingeniería y competitividad,* vol. 22, nº 2, 2020.

[18] D. Galarza , L. Barona y J. Torres, «estrategia para la evaluación de vulnerabilidades del sistema de notas de instituciones educativas utilizando técnicas de hacking ético. Caso de estudios: Instituto Tecnológico Quito,» Escuela Politécnica Nacional, Quito, 2020.

[19] E. Crespo, «Análisis de vulnerabilidades con sqlmap aplicada a entornos APEX 5,» Ingenius Revista de Ciencia y Tecnología, Cuenca, 2020.

[20] A. Alexei y A. Alexei, «Cyber Security Threat Analysis In Higher Education Institutions As A Result Of,» *International Journal of Scientific & Technology Research,* p. 8, 2021.

[21] K. García, «Implementación de la aplicación de hacking ético mediante test de intrusión “pentesting” para la detección y análisis de vulnerabilidades en la red inalámbrica de una institución educativa de la provincia de Santa Elena,» Universidad Estatal Peninsula de Santa Elena, Santa Elena, 2021.

[22] A. Izana y H. Bayu, «Information System Security Analysis to Determine Server Security Vulnerability with Penetration Testing Execution Standard (PTES) Method at VWX University,» *2021 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS),* p. 6, 2021.

[23] Á. Castillo y J. Hidalgo, «Pruebas de penetración para la seguridad informática al servidor web del laboratorio de ciberseguridad en la Universidad Politécnica Estatal del Carchi,» Universidad Politécnica Estatal del Carchi, Tulcán, 2021.

[24] C. Villalva y I. Ruíz, «análisis de las vulnerabilidades de la red LAN del distrito de educación 12D02 Puebloviejo-Urdaneta,» Babahoyo, 2021.

[25] E. Setiawan y A. Setiyadi, «Web vulnerability analysis and implementation,» IOP Conference Series: Materials Science and Engineering, Indonesia, 2018.

[26] G. Rincon y F. Albarracin, «análisis y evaluación de la seguridad informática para la página web publicada en hosting gratuito de la Institución Técnica de Firavitoba para la detección y remediación de vulnerabilidades y riesgos en la información.,» Universidad Nacional Abierta y a Distancia –UNAD, Sogamoso, 2018.

[27] R. Robles, «Análisis de vulnerabilidades, amenazas y ataques a la página web de la Universidad Técnica de Machala,» *Universidad Técnica de Machala,* p. 32, 2019.

[28] J. Delgado y R. Minaya, «Análisis de seguridad mediante metodología OWASP a redes innalambricas en Universidad Laica Eloy Alfaro de Manabí extensión en el Carmen,» *Uleam,* p. 94, 2020.

[29] C. Vega-Oyola, E. Tapia y F. Gallardo, «Análisis de factores de seguridad informática mediante la metodología OWASP v4.2: Caso de estudio ISTJOL,» *Espíritu Emprendedor TES,* vol. 6, nº 1, p. 19, 2022.

[30] J. González, «En se despliega una auditoria de seguridad informática para la institución educativa departamental Luis Carlos Galán - Municipio de Yacopí Cundinamarca,» La Dorada , 2017.

[31] C. Conforme, «Diseño de un modelo de gestión de seguridad de la información para el sistema académico de la Universidad Estatal del Sur de Manabí,» UNIVERSIDAD INTERNACIONAL SEK, Manabí, 2018.

[32] A. Bach, «Diseño de un sistema de gestión de seguridad de a información, para los procesos académicos de la Universidad Nacional de Piura,» Universidad Nacional de Piura, Piura, 2019.

[33] E. Rosales, R. Martelo y D. Franco, «diseño de un sistema de gestión de seguridad de la información para el proceso de gestión de la infraestructura tecnológica de instituciones académicas basado en la herramienta de gestión de riesgo Magerit,» *Universitaria Rafael Núñez,* 2020.

[34] C. Alvino, «Estadísticas de la situación digital de Ecuador en el 2020-2021,» *Marketing Digital,* pp. https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-de-ecuador-en-el-2020-2021/, 5 mayo 2021.

9 Anexos

ANEXO A

Cuenca 30 de junio de 2022

Mgtr.
Boris Chumbi
Rector Encargado del Instituto Superior Tecnológico del Azuay

En su despacho

Reciba un cordial y atento saludo de parte de la Universidad Politécnica Salesiana (UPS). La presente tiene la intención de poner en su conocimiento que los estudiantes **José Fabián Chuqui Quille** con cédula de ciudadanía **0104134390** y **Daniel Alejandro Orellana Gonzáles** con cédula de ciudadanía **0104418041** se encuentran matriculados en la Maestría de Seguridad de la Información y se les ha asignado el tema de trabajo de titulación intitulado **"Análisis de vulnerabilidades de seguridad de la información académica del Instituto Tecnológico del Azuay"**. En virtud de lo expuesto, solicito a usted, de la manera más atenta, se digne conceder acceso a la información de la institución que los estudiantes requieran para que la utilicen única y exclusivamente durante el desarrollo de mencionado trabajo. Conocedores de la importancia que representa la seguridad de los datos, desde la Dirección de la Maestría garantizamos la total confidencialidad y la no divulgación de la información que identifique a la institución por canal de comunicación alguno (físico o digital). De la misma manera, ruego hacernos llegar dicha autorización por escrito para el respectivo proceso académico interno de la Universidad Politécnica Salesiana.

Seguro de contar con su favorable acogida a la presente, anticipo mis agradecimientos.

Atentamente,

Miguel Arcos

Firmado digitalmente por Miguel Arcos
Nombre de reconocimiento (DN): cn=Miguel Arcos, o=UPS, ou=UPS, email=marcos@ups.edu.ec, c=EC
Fecha: 2022.06.30 15:43:30 -05'00'

Ing. Miguel Arcos Argudo, PhD.
Director Nacional de la Maestría en Seguridad de la Información
Universidad Politécnica Salesiana

VICERRECTORADO DE POSGRADO

Turuhuayco 3-69 y Calle Vieja. PBX: (+593 7) 2050000 Ext.1120 FAX: 4088958 Casilla Postal 2074
www.ups.edu.ec Cuenca - Ecuador

ANEXO B

Instituto Superior Tecnológico del Azuay

Oficio Nro. R-ISTA-2022-012
Cuenca, 04 de julio de 2022

Ing. Miguel Arcos Argudo, PhD.
Director Nacional de la Maestría en Seguridad de la Información
Universidad Politécnica Salesiana

De mi consideración:

Reciba un cordial saludo, en respuesta a su oficio s/n de fecha 30 de junio de 2022, mediante el cual se solicita acceso a la información de los estudiantes del Instituto Superior Tecnológico del Azuay con fines educativos para el trabajo de titulación de maestría para los señores José Fabián Chuqui Quille y Daniel Alejandro Orellana Gonzáles, me permito indicar que tomando en consideración la vulnerabilidad de la información de nuestra institución y de los estudiantes, se autoriza el acceso y manejo de dicha información, siempre que exista el compromiso de confidencialidad y no divulgación por ningún medio de los datos obtenidos durante el periodo académico, precautelando la seguridad e integridad de esta institución.

Con sentimientos de consideración y estima,

Atentamente,

BORIS ANIBAL
CHUMBI FLORES

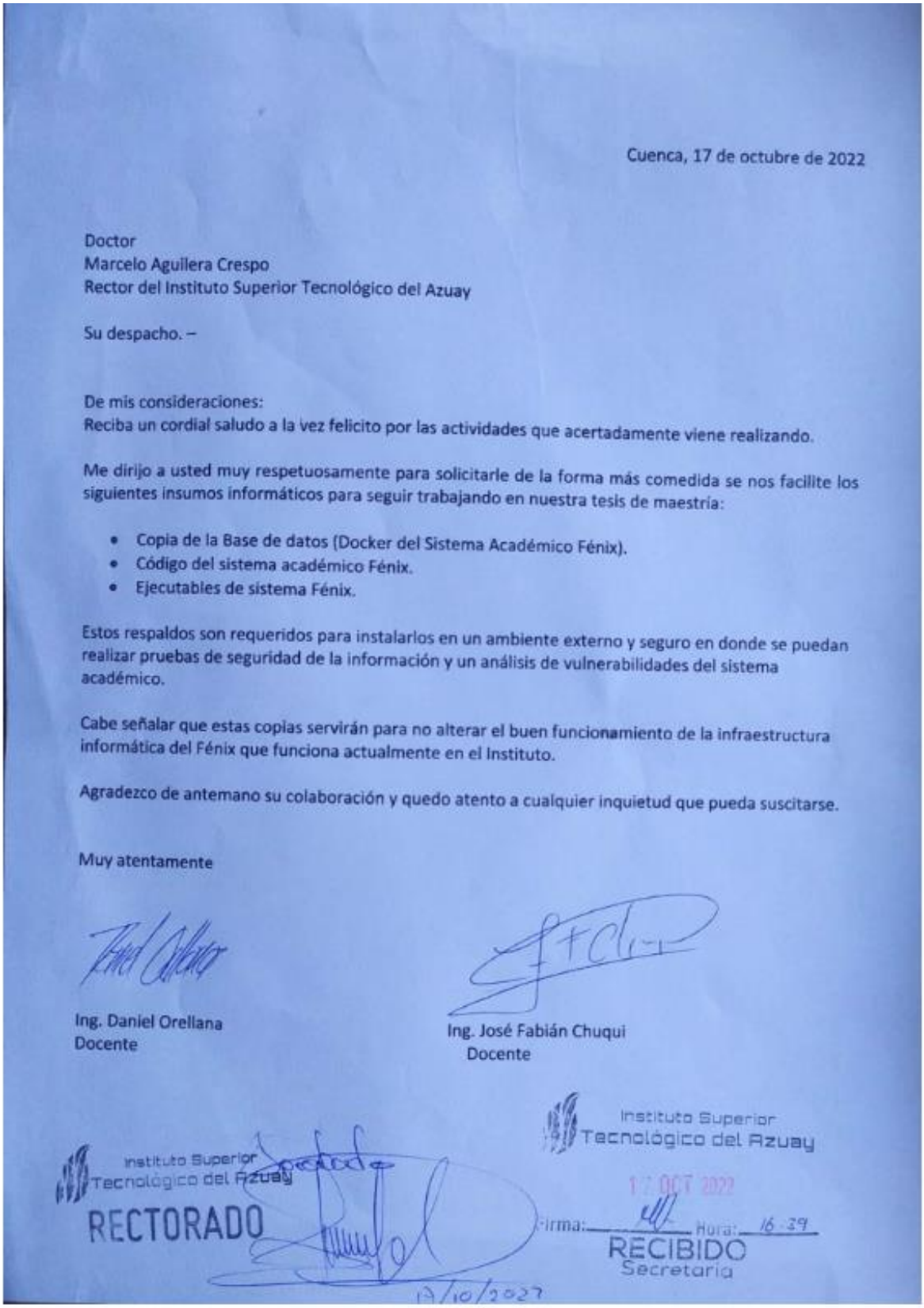
Mgtr. Boris Chumbi
RECTOR (E)
INSTITUTO SUPERIOR TECNOLÓGICO DEL AZUAY

Instituto Superior Tecnológico del Azuay

Dirección: Av. Octavio Chacón 198 y Primera Transversal. Teléfono: (07) 2809-551
Celular: 0995363076 email: secretaria.istazuay@gmail.com
Cuenca – Ecuador

1 de 1

ANEXO C



Cuenca, 17 de octubre de 2022

Doctor
Marcelo Aguilera Crespo
Rector del Instituto Superior Tecnológico del Azuay

Su despacho. –

De mis consideraciones:
Reciba un cordial saludo a la vez felicito por las actividades que acertadamente viene realizando.

Me dirijo a usted muy respetuosamente para solicitarle de la forma más comedida se nos facilite los siguientes insumos informáticos para seguir trabajando en nuestra tesis de maestría:

- Copia de la Base de datos (Docker del Sistema Académico Fénix).
- Código del sistema académico Fénix.
- Ejecutables de sistema Fénix.

Estos respaldos son requeridos para instalarlos en un ambiente externo y seguro en donde se puedan realizar pruebas de seguridad de la información y un análisis de vulnerabilidades del sistema académico.

Cabe señalar que estas copias servirán para no alterar el buen funcionamiento de la infraestructura informática del Fénix que funciona actualmente en el Instituto.

Agradezco de antemano su colaboración y quedo atento a cualquier inquietud que pueda suscitarse.

Muy atentamente

Ing. Daniel Orellana
Docente

Ing. José Fabián Chuqui
Docente

Instituto Superior Tecnológico del Azuay
RECTORADO
19/10/2022

Instituto Superior Tecnológico del Azuay
17 OCT 2022
Firma: Hora: 16:39
RECIBIDO
Secretaría

ANEXO D1

COMPROMISO DE CONFIDENCIALIDAD, NO DIVULGACIÓN DE LA INFORMACIÓN Y BUEN USO DEL SOFTWARE

Yo, DANIEL ALEJANDRO ORELLANA GONZALEZ , de nacionalidad ECUATORIANA, con documento de identidad número 0104418041 , como Servidor/a Público y en calidad de DOCENTE , bajo la modalidad contractual de SERVICIOS OCACIONALES; que a efecto de este compromiso se me denominará como "EL FUNCIONARIO/SERVIDOR/TRABAJADOR", conozco la importancia de la información a la que tendré acceso y gestionaré mediante el repositorio de información que se manejen en el Instituto Superior Tecnológico del Azuay con condición de Universitario, para lo cual me comprometo al cumplimiento del siguiente instrumento tomando en cuenta lo siguiente:

PRIMERA. - BASE LEGAL Y ANTECEDENTES

1.1. La Constitución de la República del Ecuador, preceptúa:

"Art. 18.- Todas las personas, en forma individual o colectiva, tienen derecho a: (...)
2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información.

"Art. 66.- Se reconoce y garantizará a las personas: (...)
19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la Ley"

TEC AZUAY
INSTITUTO UNIVERSITARIO

1.2. Ley Orgánica de Transparencia y Acceso a la Información Pública establece:

"Art. 5.- Información Pública. - Se considera información pública, todo documento en cualquier formato, que se encuentre en poder de las instituciones públicas y de las personas jurídicas a las que se refiere esta Ley, contenidos, creados u obtenidos por ellas, que se encuentren bajo su responsabilidad o se hayan producido con recursos del Estado."

"Art. 6.- Información Confidencial. - Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, (...). El uso ilegal que se haga de la información personal o su divulgación, dará lugar a las acciones legales pertinentes. No podrá invocarse reserva, cuando se trate de investigaciones que realicen las autoridades públicas competentes, sobre violaciones a derechos de las personas que se encuentren establecidos en la Constitución Política de la República, en las declaraciones, pactos, convenios, instrumentos internacionales y el ordenamiento jurídico interno. Se excepciona el procedimiento establecido en las indagaciones previas."

"Art. 9.- Responsabilidad sobre la entrega de la Información Pública. - El titular de la entidad o representante legal, será el responsable y garantizará la atención suficiente y necesaria a la publicidad de la información pública, así como su libertad de acceso. Su responsabilidad será recibir y contestar las solicitudes de acceso a la información, en el plazo perentorio de diez días, mismo que puede prorrogarse por cinco días más, por causas debidamente justificadas e informadas al peticionario."

"Art. 19.- De la Solicitud y sus Requisitos. - El interesado a acceder a la información pública que reposa, manejan o producen las personas jurídicas de derecho público y demás entes señalados en el artículo 1 de la presente Ley, deberá hacerlo mediante solicitud escrita ante el titular de la institución. En dicha solicitud deberá constar en forma clara la identificación del solicitante y la ubicación de los datos o temas motivo de la solicitud, la cual será contestada en el plazo señalado en el artículo 9 de esta Ley."

1.3. El Código Integral Penal tipifica:

"Art. 233.- Delitos contra la información pública reservada legalmente. - La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años. La o el

servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años. Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad".

"Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años".

"Art. 310.- Divulgación de información financiera reservada. - La persona que, en beneficio propio o de terceros, divulgue información financiera declarada como reservada por el ente rector de finanzas públicos, que genere condiciones económicas desfavorables para el Estado, será sancionada con pena privativa de libertad de tres a cinco años".

1.4. La Ley del Sistema Nacional de Registro de Datos Públicos dispone:

"Art. 4.- Los instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva de la o el declarante cuando esta o este provee toda la información..."

"Art. 6.- Accesibilidad y confidencialidad. - Son confidenciales los datos de carácter personal, tales como: ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria y los demás atinentes a la intimidad personal y en especial aquella información cuyo uso público atente

contra los derechos humanos consagrados en la Constitución e instrumentos internacionales. El acceso a estos datos sólo será posible con autorización expresa del titular de la información, por mandato de la ley o por orden judicial. También son confidenciales los datos cuya reserva haya sido declarada por la autoridad competente, los que estén amparados bajo sigilo bancario o bursátil, y los que pudieren afectar la seguridad interna o externa del Estado. La autoridad o funcionario que por la naturaleza de sus funciones custodie datos de carácter personal, deberá adoptar las medidas de seguridad necesarias para proteger y garantizar la reserva de la información que reposa en sus archivos."

1.5. El Esquema Gubernamental de Seguridad de la Información (EGSI V2), en sus numerales 3 y 9 señala:

3.1.2 Términos y condiciones laborales
Control
"Los funcionarios, contratistas y terceros deben aceptar y firmar los términos y condiciones del contrato de trabajo, el cual establece sus responsabilidades y obligaciones de acuerdo a la norma legal vigente.
3.1.2.1 Realizar la firma del acuerdo de confidenciolidad o no-divulgación, antes de que los empleados, contratistas y usuarios de terceras partes, tengan acceso a la información. Dicho acuerdo debe establecer los parámetros tanto de vigencia del acuerdo, información confidencial referida, formas de acceso, responsabilidades y funciones.
3.1.2.2 Socializar los derechos y responsabilidades legales de los empleados, los contratistas y cualquier otro usuario sobre la protección de datos y derechos de propiedad intelectual; dejando constancia de lo actuado a través de hojas de registro, informes o similares, que evidencie la realización de la misma.
3.1.2.3 Responsabilizar al personal o contratistas por la clasificación de la información y la gestión de la información de la institución y de otros activos relacionados con la información, instalaciones de procesamiento de la información y a los servicios de información
3.1.2.4 Responsabilizar al personal sobre el manejo y creación de la información tanto interna como externa, resultante durante la ejecución de la relación laboral establecida con la institución;
3.1.2.5 Comunicar al personal o contratista las acciones legales que se tomaran si hace caso omiso de cumplir con las normas legales vigentes en la institución."

9.2.4 Acuerdos de confidencialidad o no revelación
Control

"Elaborar el acuerdo de confidencialidad observando los requisitos que deben ser parte del mismo, considerando la no divulgación de la información de acuerdo a la necesidad de la institución.

9.2.4.1 Determinar la duración prevista del acuerdo, incluyendo los casos en los que la confidencialidad necesite mantenerse indefinidamente;

9.2.4.2 Responsabilidades y acciones de los firmantes para evitar la revelación no autorizada de la información;

9.2.4.3 Propiedad intelectual de la información, considerar de acuerdo a las directrices de la clasificación de la información.

9.2.4.4 Implementar políticas para el uso de la información confidencial permitida.

9.2.4.5 Definir claramente el derecho de auditar y supervisar las actividades que involucren con la gestión de información en los equipos institucionales y que naveguen en la red de la institución.

9.2.4.6 Acciones que pueden ser tomadas en caso de incumplimiento del acuerdo, de acuerdo a la norma legal vigente.

9.2.4.7 Definir las acciones necesarias cuando se termine un acuerdo.

9.2.4.8 Definir procesos para notificación y aviso de la difusión no autorizada o fugas de información confidencial;

9.2.4.9 Elaborar y aprobar los acuerdos de confidencialidad y de no-divulgación de información conforme la Constitución, las leyes, las necesidades de protección de información de la institución y el EGSI.

9.2.4.10 Controlar que los acuerdos de confidencialidad de la información, documento físico o electrónico, sean firmados de forma manuscrita o electrónica por todo el personal de la institución sin excepción.

9.2.4.11 Gestionar la custodia de los acuerdos firmados, en los expedientes, físicos o electrónicos, de cada funcionario, por parte del área de gestión de recursos humanos.

9.2.4.12 Controlar que la firma de los acuerdos de confidencialidad sean parte de los procedimientos de incorporación de nuevos funcionarios a la institución, sin excepción.

9.2.4.13 Gestionar la aceptación, entendimiento y firma de acuerdos de confidencialidad y de no divulgación de información por parte de terceros (ej., contratistas, proveedores, pasantes, entre otros) que deban realizar labores dentro de la institución sea por medios lógicos o físicos y que involucren el manejo de información."

2.- SEGUNDA.- Propiedad de la Información.

2.1.- "EL FUNCIONARIO/SERVIDOR/TRABAJADOR", reconoce el derecho de propiedad de la Información que mantiene el Instituto Superior Tecnológico del

Azuay con condición de Universitario, incluyendo y sin limitarse, a la que puede ser accedida mediante el servicio de GOOGLE DRIVE, FENIX, SIGA, y más aplicaciones que se desarrollaran o a las que "EL FUNCIONARIO/SERVIDOR/TRABAJADOR" tuviera acceso. En tal virtud, "EL FUNCIONARIO/SERVIDOR/TRABAJADOR", renuncia a reclamar cualquier derecho de propiedad sobre la misma.

Por tanto, "EL FUNCIONARIO/SERVIDOR/TRABAJADOR" se compromete a entregar en cualquier momento toda la información obtenida mediante estos servicios y más aplicaciones que se creasen o a las que tuviera acceso, debiendo este guardar para sí, respaldo por cualquier medio sea este digital o impreso de la información por el/ella generado, encargada.

"EL FUNCIONARIO/SERVIDOR/TRABAJADOR" se obliga en forma irrevocable ante el Instituto Superior Tecnológico del Azuay con condición de Universitario a no revelar, divulgar o facilitar bajo cualquier forma- a persona alguna sea natural o jurídica, pública o privada, o de cualquier otra naturaleza, y a no utilizar para su propio beneficio o para beneficio de un tercero, toda la información generada durante la vigencia de su correspondiente contrato, nombramiento, etc.

Queda expresamente acordado entre las partes que no se podrá modificar, hacer pública, divulgar o utilizar de cualquier forma conocida o por conocerse a terceros o para su propio beneficio o para beneficio de cualquier otra persona natural o jurídica, la información objeto del presente Acuerdo sin previa autorización escrita y expresa por la Autoridad competente, o en aquellos casos en los que la ley faculta o dispone a "EL FUNCIONARIO/SERVIDOR/TRABAJADOR" a entregar a terceros aquella información que esté sujeta a sigilo o reserva.

2.2.- Información Confidencial.- Para efectos de este compromiso se entiende como información confidencial y extremadamente sensible, todos los hechos o antecedentes que no han sido divulgados al público general de manera oficial por parte de la SENESCYT o el Instituto Superior Tecnológico del Azuay con condición de Universitario, sin importar que dicha información conste en documentos físicos, archivos informáticos, mensajes electrónicos o cualquier otro soporte material o que hayan sido conocidos por el servidor por cualquier medio.

2.3.- Divulgación Oficial.- se entiende a la información que es entregada al público por parte del Instituto Superior Tecnológico del Azuay con condición de Universitario, a través de declaraciones públicas; boletines oficiales de prensa u otro tipo de publicaciones efectuadas por la institución con la autorización de las autoridades, a través de medios de comunicación y/o medios electrónicos, de acuerdo con la ley y normas legales vigentes.

3.- **TERCERA**.- Objeto.

El presente Acuerdo tiene por objeto mantener en forma estrictamente reservada y confidencial la información que goza de confidencialidad y se la considera de carácter sensible que fue proporcionada a las/os FUNCIONARIOS/SERVIDORES/TRABAJADORES; así como, la información que es obtenida de los medios antes descritos y más aplicaciones que se creasen o a las que las/os FUNCIONARIOS/SERVIDORES/TRABAJADORES tuvieran acceso, sin importar el medio físico o electrónico en el que se encuentre almacenada. A su vez, se encuentra protegida por los lineamientos de este instrumento, así como de las disposiciones de carácter legal contempladas en la legislación nacional vigente.

4.- **CUARTA**.- Confidencialidad

En atención a la naturaleza de la información y los riesgos que provienen del mal uso y/o divulgación de la misma, que pueden implicar a la SENESCYT o al Instituto Superior Tecnológico del Azuay con condición de Universitario, "EL FUNCIONARIO/SERVIDOR/TRABAJADOR" se compromete a mantener absoluta reserva de la información a la que tenga acceso; además se obliga a abstenerse de usar, disponer, divulgar, transferir y/o publicar por cualquier medio, oral o escrito, compartir su contenido o enlaces a personas internas o externas no autorizadas para acceder o recibir información, y en general, aprovecharse de ella de cualquier forma para efectos ajenos y que se vayan en contra de la SENESCYT y el Instituto Superior Tecnológico del Azuay con condición de Universitario, durante y por un plazo de cinco años contados a partir de que finalice la prestación de sus servicios en la institución, sin perjuicio del plazo de responsabilidad que establezca la Ley Orgánica de, Servicio Público o similares.

"EL FUNCIONARIO/SERVIDOR/TRABAJADOR" se compromete a abstenerse de realizar para sí o para terceros, copias, enlaces, arreglos, reproducciones, adaptaciones, mutilaciones, deformaciones del contenido alojado las herramientas antes definidas y más aplicaciones que se creasen o a las que "EL FUNCIONARIO/SERVIDOR/TRABAJADOR" tuviera acceso.

"EL FUNCIONARIO/SERVIDOR/TRABAJADOR" se compromete a mantener en absoluto secreto sus credenciales personales de acceso (usuario y contraseña) a las herramientas descritas y más aplicaciones que se creasen o a las que "EL FUNCIONARIO/SERVIDOR/TRABAJADOR" tuviera acceso, absteniéndose de compartirlas, divulgarlas o escribirlas en lugares visibles o accesibles por otras personas. En caso de que, por razones ajenas a su voluntad, las credenciales personales de acceso de "EL FUNCIONARIO/SERVIDOR/TRABAJADOR" hubieran

sido vulneradas o divulgadas a terceras personas, "EL FUNCIONARIO/SERVIDOR/TRABAJADOR" está obligado a notificar inmediatamente a la Dirección de Soporte Tecnológico o quien haga sus veces, con copia a Rectorado. Esto incluye, pero sin limitarse, al robo, hurto o extravío de su equipo de computación personal o laboral, teléfono celular y todo dispositivo o soporte físico o magnético en el que hubiera almacenado las credenciales personales de acceso o, en general, información de institucional. Además, "EL FUNCIONARIO/SERVIDOR/TRABAJADOR" se compromete a mantener íntegra la información recibida, en la carpeta individual asignada a su usuario, y entregarla al Instituto, a través del director, Coordinador o jefe de las unidades a las que perteneció durante su período de labores, de forma oportuna e inmediata, cuando esta lo requiera y al finalizar su relación laboral o contractual con la institución.

Adicionalmente, "EL FUNCIONARIO/SERVIDOR/TRABAJADOR" se compromete a guardar en su totalidad en GOOGLE DRIVE y más aplicaciones que se creasen o a las que "EL FUNCIONARIO/SERVIDOR/TRABAJADOR" tuviera acceso, toda la información a su cargo cuando cambie de funciones o sea asignado a otra unidad administrativa.

En caso de incumplir con dicho compromiso se someterá a las sanciones contenidas en el ordenamiento jurídico vigente. "EL FUNCIONARIO/SERVIDOR/TRABAJADOR"; además tiene la obligación ética y moral de informar cualquier actuación o conducta sospechosa en desmedro de la institución, de nuestro Código de Ética o de nuestra comunidad académica en general.

5.- **QUINTA** .- Propiedad Intelectual.

El Instituto Superior Tecnológico del Azuay con condición de Universitario es propietaria de toda la información, de la cual se encuentra prohibida su publicación y/o divulgación, toda clase de documentos, archivos e información que se encuentren en soportes físicos o electrónicos, así como registros, diagramas, flujogramas, dibujos, fotografías, disposiciones internas, memorándums, programas para computadora desarrollados al interior de la entidad, creaciones en multimedia o equipos digitales, logotipos, ideas, proyectos y en general toda clase de datos que se generen en la entidad, como parte de sus labores.

Se considera protegida por esta cláusula a toda la información, productos y servicios generados por los funcionarios y servidores públicos, personas naturales y jurídicas, públicas y privadas, relacionados con la institución, siendo estas de propiedad exclusiva del Instituto Superior Tecnológico del Azuay con condición de Universitario, de acuerdo con las disposiciones contenidas en Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, por lo que los derechos de propiedad intelectual de la información que pertenecen al Instituto Superior Tecnológico del Azuay con condición de Universitario no podrán ser revelados por "EL FUNCIONARIO/SERVIDOR/TRABAJADOR" para su reproducción parcial o total; así como su comunicación pública y distribución, sin el consentimiento previo y debida autorización de su titular

Cualquier falta a estas obligaciones y/o utilice la información para beneficio particular o de terceros será causa suficiente para considerar que la/el FUNCIONARIO/SERVIDOR/TRABAJADOR, ha incumplido el presente compromiso y puede dar lugar a que la SENESCYT o el Instituto Superior Tecnológico del Azuay con condición de Universitario inicie las acciones legales pertinentes conforme a la normativa legal vigente.

6.- **SEXTA**.- Excepciones.

"EL FUNCIONARIO/SERVIDOR/TRABAJADOR" no tendrá deber alguno de confidencialidad en los siguientes casos:

i. Cuando la información sea de dominio o conocimiento público.
ii. Cuando en base a lo establecido en la normativa vigente, deje de ser considerada como información confidencial, y a su vez sea conocido por la(s) autoridad(es) competente(s) del Instituto Superior Tecnológico del Azuay con condición de Universitario.
iii. En concordancia con el punto anterior la información que sea considerada pública por la Ley Orgánica de Transparencia y Acceso a la Información Pública.
iv. Cuando la Información deje de ser confidencial, al ser revelada por el personal debidamente autorizado por parte del Instituto Superior Tecnológico del Azuay con condición de Universitario.

7.- **SÉPTIMA**. - Sanciones.

"EL FUNCIONARIO/SERVIDOR/TRABAJADOR" acepta y reconoce que la información del Instituto Superior Tecnológico del Azuay con condición de

Universitario constituye un bien intangible invaluable, por lo que el mal uso o la falta de cumplimiento de su compromiso de confidencialidad atraerá la imposición de sanciones de índole administrativa, civil y penal, constantes en el ordenamiento legal vigente, sin perjuicio de la aplicación del régimen disciplinario y las acciones que, por su parte, pueda seguir la SENESCYT y/o el Instituto Superior Tecnológico del Azuay con condición de Universitario.
Las sanciones administrativas a imponerse se determinarán por la gravedad de la falta y conforme a lo establecido en la Ley Orgánica del Servicio Público, su Reglamento General, COA, el Reglamento Interno de Administración del Talento Humano de la SENESCYT y/o el Reglamento Disciplinario del Instituto Superior Tecnológico del Azuay con condición de Universitario, estas son:

1. Amonestación verbal
2. Amonestación escrita
3. Sanción pecuniaria administrativa
4. Suspensión Temporal sin goce de Remuneración; y,
5. Destitución

Sin perjuicio de lo estipulado y si la mala utilización o manejo de que la información causare un daño, inmediato e irreparable a la SENESCYT y/o el Instituto Superior Tecnológico del Azuay con condición de Universitario o a los organismos bajo su control, queda expresamente aceptado por el firmante, facultar afinan la SENESCYT y al Instituto Superior Tecnológico del Azuay con condición de Universitario para disponer la terminación del contrato de trabajo con justa causa. Asimismo, la SENESCYT y este Instituto Superior Tecnológico del Azuay con condición de Universitario queda facultado para accionar por daños y perjuicios efectivamente ocasionados y comprobados, así como para constituirse en parte demandante de una denuncia penal o acciones civiles y administrativas contra "EL FUNCIONARIO/SERVIDOR/TRABAJADOR".

8.- **OCTAVA**.- Duración.

"EL FUNCIONARIO/SERVIDOR/TRABAJADOR" se compromete a guardar la confidencialidad del contenido de la información expresada en el presente acuerdo y que llegare a su conocimiento por cualquier medio. No obstante, su compromiso permanecerá vigente por un periodo de cinco años luego de terminada su relación contractual o laboral con la SENESCYT y/o el Instituto Superior Tecnológico del Azuay con condición de Universitario.

9.- **NOVENA**. Controversias.

En caso de que la SENESCYT y/o el Instituto Superior Tecnológico del Azuay con condición de Universitario considere que existe un incumplimiento por parte de "EL FUNCIONARIO/SERVIDOR/TRABAJADOR", en relación con las obligaciones asumidas en este instrumento, se reserva el derecho de interponer las acciones que considere pertinentes ante los juzgados y tribunales de la República del Ecuador, en las vías que correspondan; a interponer las respectivas denuncias ante la Fiscalía General del Estado; y, a ejercer la potestad administrativa sancionatoria que le confiere el Código Orgánico Administrativo. Para este propósito, "EL FUNCIONARIO/SERVIDOR/TRABAJADOR" renuncia a fuero y domicilio y acepta ser demandado en la ciudad de Cuenca.

Como constancia de lo acordado, "EL FUNCIONARIO/SERVIDOR/TRABAJADOR" suscribe el presente instrumento en dos (02) ejemplares de igual tenor, en la ciudad de Cuenca, a los 11 días del mes de noviembre del 2022.

DANIEL ALEJANDRO ORELLANA GONZALEZ
CC: 0104418041
FUNCIONARIO/SERVIDOR/TRABAJADOR

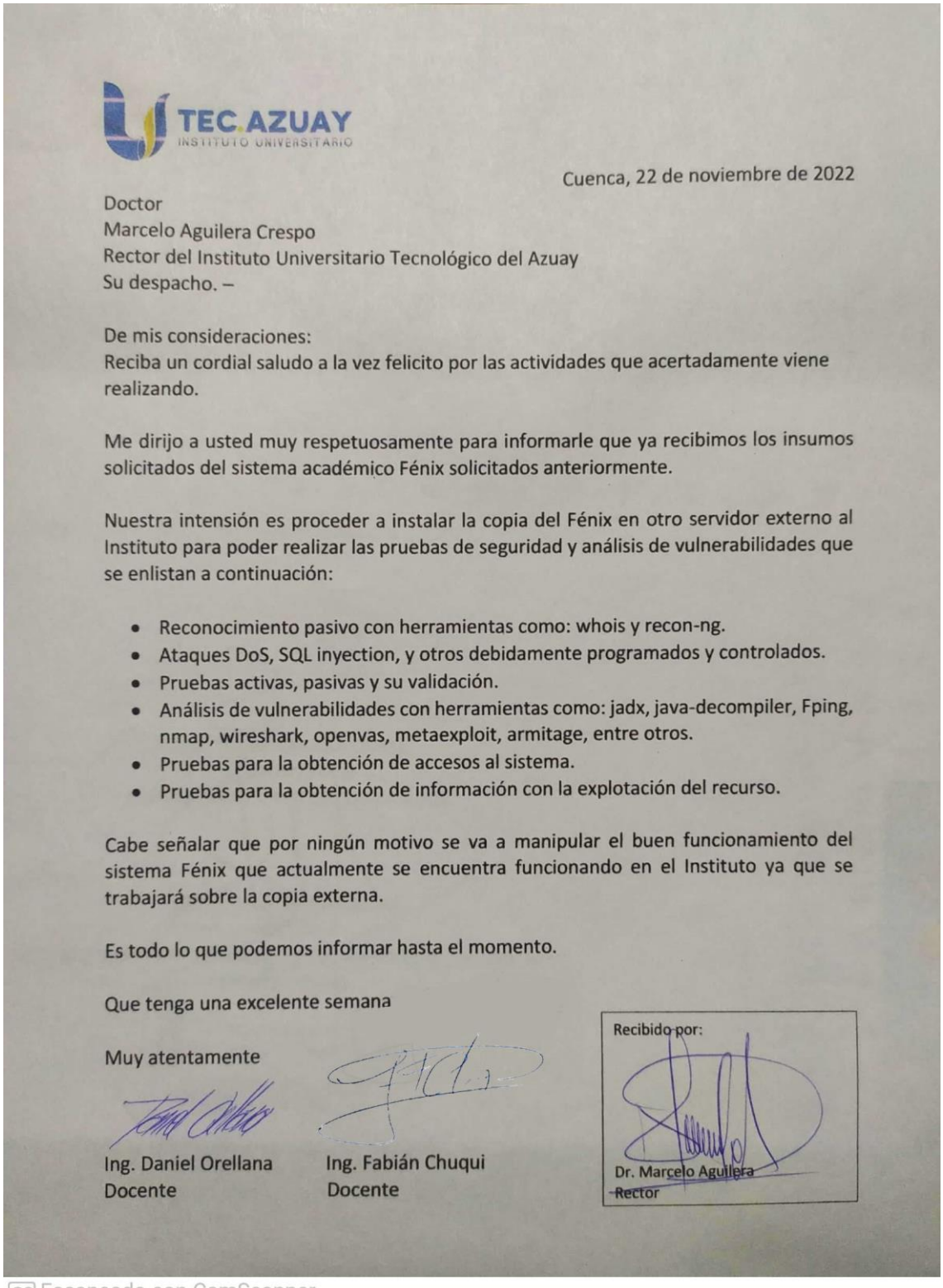
MGTR. MARCELO AGUILERA
RECTOR
INSTITUTO SUPERIOR TECNOLÓGICO DEL AZUAY CON CONDICIÓN DE UNIVERSITARIO.

Instituto Superior Tecnológico del Azuay
RECTORADO

ANEXO D2

Idéntico al anexo D1 por lo que se trata del “Compromiso de confidencialidad, no divulgación de la información y buen uso del software“ firmado por Fabián Chuqui.

ANEXO E



TEC.AZUAY
INSTITUTO UNIVERSITARIO

Cuenca, 22 de noviembre de 2022

Doctor
Marcelo Aguilera Crespo
Rector del Instituto Universitario Tecnológico del Azuay
Su despacho. –

De mis consideraciones:
Reciba un cordial saludo a la vez felicito por las actividades que acertadamente viene realizando.

Me dirijo a usted muy respetuosamente para informarle que ya recibimos los insumos solicitados del sistema académico Fénix solicitados anteriormente.

Nuestra intensión es proceder a instalar la copia del Fénix en otro servidor externo al Instituto para poder realizar las pruebas de seguridad y análisis de vulnerabilidades que se enlistan a continuación:

- Reconocimiento pasivo con herramientas como: whois y recon-ng.
- Ataques DoS, SQL inyection, y otros debidamente programados y controlados.
- Pruebas activas, pasivas y su validación.
- Análisis de vulnerabilidades con herramientas como: jadx, java-decompiler, Fping, nmap, wireshark, openvas, metaexploit, armitage, entre otros.
- Pruebas para la obtención de accesos al sistema.
- Pruebas para la obtención de información con la explotación del recurso.

Cabe señalar que por ningún motivo se va a manipular el buen funcionamiento del sistema Fénix que actualmente se encuentra funcionando en el Instituto ya que se trabajará sobre la copia externa.

Es todo lo que podemos informar hasta el momento.

Que tenga una excelente semana

Muy atentamente

Ing. Daniel Orellana
Docente

Ing. Fabián Chuqui
Docente

Recibido por:

Dr. Marcelo Aguilera
Rector

ANEXO F

MARCO DE POLITICAS PROPUESTO PARA EL CONTROL DE LA SEGURIDAD DEL SISTEMA FÉNIX		
REFERENCIA CONTROL	**POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN SEGÚN ISO 27002:2022**	**DETALLE DE LA POLÍTICA A IMPLEMENTAR EN EL SISTEMA FÉNIX**
6.6	Acuerdos de confidencialidad o no divulgación	**Políticas de Relación laboral** El Departamento de recursos humanos deberá presentar a trabajadores, docentes y empleados del Instituto la suscripción de un acuerdo de confidencialidad, no divulgación de la información y uso adecuado de los sistemas de información.
5.11	Devolución de activos	**Políticas de Relación laboral** Los trabajadores que se desvinculen de la Institución deberán participar en un proceso bien establecido en donde se lleve a cabo la devolución de activos de información, el cierre y bloqueo de todos sus accesos y el borrado de datos de información institucional.
5.9	Inventario de información y otros activos asociados	**Políticas de Gestión de Activos de Seguridad** El departamento de TIC en trabajo conjunto con las coordinaciones y jefaturas del Instituto deberán mantener un inventario actualizado de los activos de información y su respectivo responsable. El responsable del activo de seguridad de la información deberá asegurar su buen uso, custodia y protección. Los activos se utilizarán bajo los acuerdos y reglamentaciones vigentes.
5.10	Uso aceptable de la información y otros activos asociados	
5.12	Clasificación de la información	**Políticas para la clasificación y etiquetado de documentos** Los documentos digitales y físicos deberán ser clasificados y etiquetados según los siguientes tipos: Documentación pública,

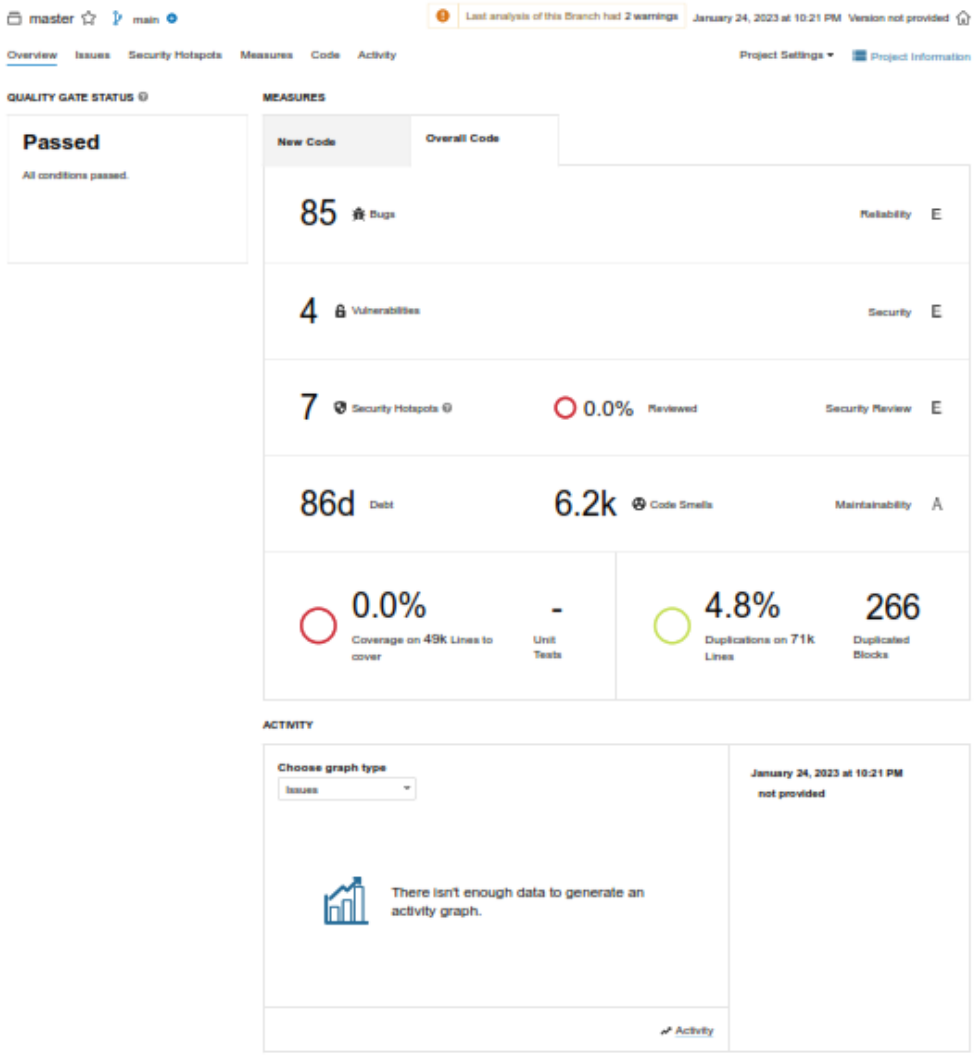
5.13	Etiquetado de la información	documentación interna y documentación confidencial. • Documentación publica: Información disponible para la colectividad en general. • Documentación interna: Información usada y reconocida por usuarios internos. • Documentación confidencial: Información que está avalada por un autor o propietario y que debe ser autorizada para su publicación.
8.7	Protección contra el malware	**Políticas de protección antimalware** Las políticas también buscan proteger a los activos se seguridad de la información de infecciones de software malicioso. Las políticas para este apartado son: • La Unidad de TIC deberá implementar soluciones antimalware en todos los equipos informáticos del Instituto. • La Unidad de TIC deberá realizar análisis periódicos de software malicioso con un sistema antimalware. • La herramienta antimalware deberán ser capaz de prevenir y detectar software malicioso. • La herramienta antimalware deberá ser capaz de mantener actualizados sus registros y componentes.
5.14	Transferencia de información	**Políticas sobre el uso de internet, correos electrónicos y mensajería.** Las políticas que aplican al uso del internet, correo electrónico y mensajería son: • El uso del servicio de internet se limitará a consultas de tipo académicas, investigativas, operativas y otras relacionadas a la educación. • Las cuentas de correo institucionales serán exclusivamente utilizadas para uso institucional. • No se deberá responder o reenviar correos catalogados como spam,
8.21	Seguridad de los servicios de red	

		cadenas de mensajes y correos de remitentes desconocidos y se debe proceder a eliminarlos de forma definitiva. • La documentación interna y la documentación confidencial enviada, recibida o almacenada deberá ser gestionada solamente a través de cuentas institucionales.
5.7	Inteligencia sobre amenazas	**Política de gestión de riesgos** Los activos de la seguridad de la información críticos deberán ser incluidos en un estudio de análisis de gestión de riesgos siguiendo la metodología correspondiente en donde se identifiquen las amenazas, impacto y tratamiento de mitigación sugeridos.
6.3	Sensibilización, educación y formación en materia de seguridad de la información	**Políticas de concientización de usuarios** Ejecutar campañas de información y capacitación en donde se promuevan las buenas prácticas de seguridad de la información con el afán de crear conciencia sobre la protección y preservación de la información Institucional. Estas campañas deberán estar enfocadas a socializar las Políticas de Seguridad de la Información.
8.20	Seguridad de las redes	**Políticas de controles de seguridad** La Unidad de TIC deberá implementar configuraciones, reglas y controles de seguridad en firewall, proxy, IPSs, IDs y demás herramientas de seguridad para garantizar la protección de datos que ingresen a la red de comunicación interna de la Institución.
8.21	Seguridad de los servicios de red	
8.24	Uso de la criptografía	**Política para el cifrado de la información** La unidad de TIC deberá implementar el cifrado de la información en bases de datos y discos de almacenamiento incluyendo contraseñas de acceso. El cifrado también se debe incluir en usuarios y contraseñas de administrador o superusuario resguardando esta

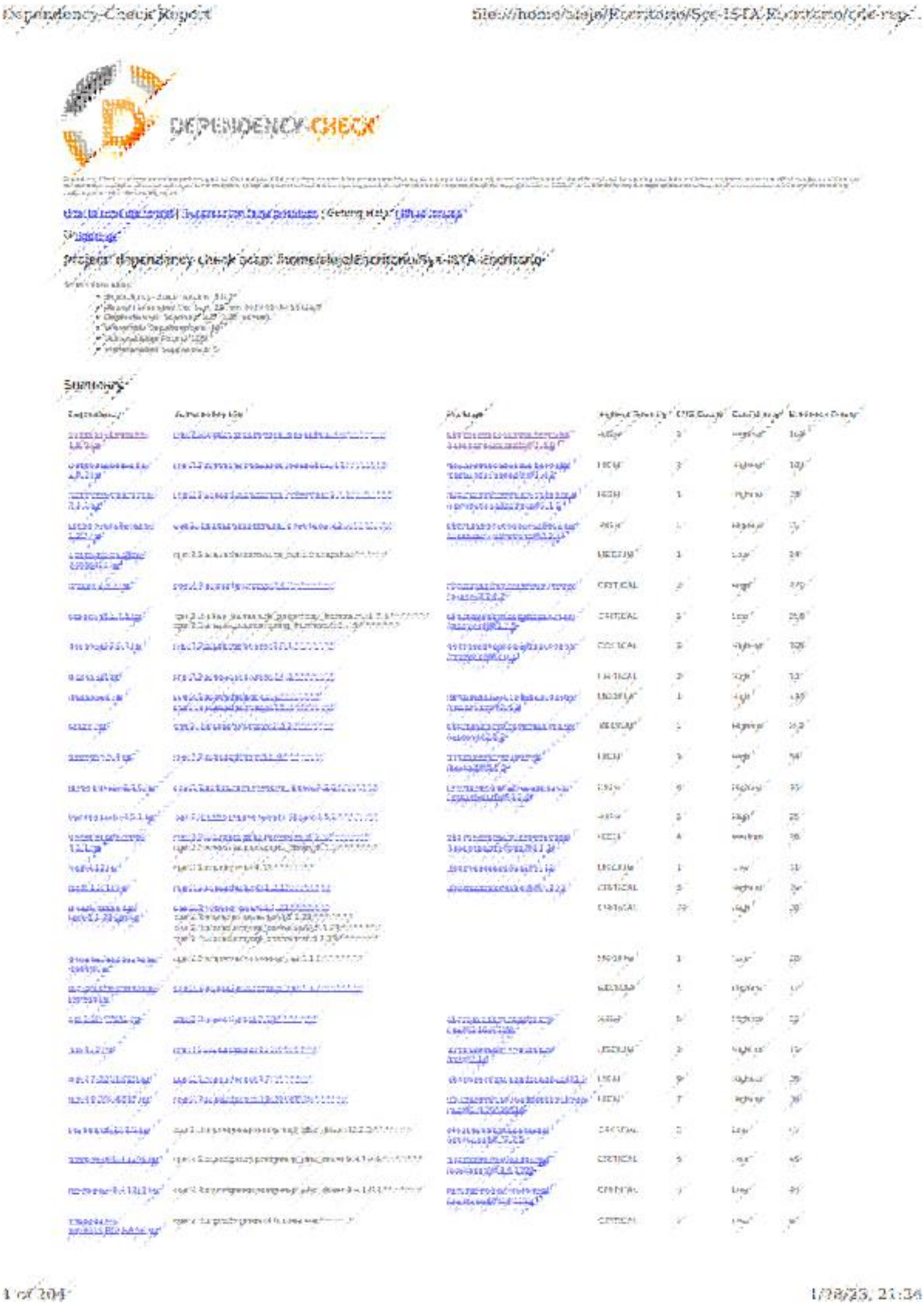
		información en lugares estratégicos y seguros de la infraestructura informática
6.8	Informes de eventos de seguridad de la información	**Política para la gestión de registros de eventos** La unidad de TIC deberá implementar un sistema de registro de eventos o pistas de auditoría para el acceso o modificaciones de la información confidencial o reservada en las aplicaciones de información. Estos eventos realizados por el usuario deberán corresponder a: • Hora y fecha de ultimo acceso o intento de acceso. • Dirección IP y otros parámetros relacionados de la máquina que se conecta. • Cambios de estado de usuario (activo, inactivo, bloqueo) • Número de intentos de acceso fallidos y exitosos. • Fecha y hora de cambio de contraseña
5.25	Evaluación y decisión sobre eventos de seguridad de la información	
5.17	Information de autentificación	**Política para la autenticación** La unidad de TIC deberá implementar un sistema centralizado de autenticación y un sistema de doble factor de autenticación para aplicaciones críticas.
		Política de contraseñas Las políticas para gestionar el uso y creación de contraseñas se definen a continuación: • Deberán disponer de una longitud de 8 caracteres. • Las contraseñas deberán contener al menos dos de los siguientes grupos de caracteres: mayúsculas, minúsculas, numéricos, especiales. • Se prohíbe usar nombres, fechas de nacimiento, domicilios o palabras de diccionario o comunes relacionadas con su identificador de usuario. • Los sistemas informáticos de la Institución deberán obligar al usuario a cambiar su contraseña en su primer ingreso.

		• Luego de 5 intentos fallidos de inicio de sesión se realizará el bloqueo de la cuenta de usuario. • Se debe especificar cambios de contraseñas de usuario mínimo cada 6 meses.
8.13	Información de respaldo	**Políticas de respaldos de seguridad** El departamento de TIC deberá contar con procedimientos aprobados para realizar copias de seguridad de la información de bases de datos, servidores, aplicaciones, código fuente, entre otros, considerando aspectos como: frecuencia, tiempo de retención, verificación, almacenamiento en una ubicación remota.
7.1	Perímetro de seguridad física	**Política de la seguridad física en las instalaciones** Las instalaciones de procesamiento de información como: centros de datos, cuartos de comunicaciones y las instalaciones del departamento de TIC, deberán contar con sistemas que garanticen el registro y control del acceso físico, con sistemas biométricos, lectores de tarjetas magnéticas o identificación por radiofrecuencia. Este sistema de control de acceso deberá mantener el histórico de accesos a estas áreas de procesamiento de información.
7.2	Entrada física	

ANEXO G


master
main
Last analysis of this Branch had 2 warnings
January 24, 2023 at 10:21 PM Version not provided
Overview
Issues
Security Hotspots
Measures
Code
Activity
Project Settings
Project Information
QUALITY GATE STATUS
Passed
All conditions passed.
MEASURES
New Code
Overall Code
85 Bugs
Reliability E
4 Vulnerabilities
Security E
7 Security Hotspots
0.0% Reviewed
Security Review E
86d Debt
6.2k Code Smells
Maintainability A
0.0%
Coverage on 49k Lines to cover
-
Unit Tests
4.8%
Duplications on 71k Lines
266
Duplicated Blocks
ACTIVITY
Choose graph type
Issues
There isn't enough data to generate an activity graph.
Activity
January 24, 2023 at 10:21 PM
not provided

ANEXO H



DEPENDENCY-CHECK

project: dependency-check scan: /home/.../Escritorio/Sys-ISTA-Escritorio

Summary

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]


Dependency-Check Report

ANEXO I

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 190.15.132.41
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-01 11:06 EST
Nmap scan report for 190.15.132.41
Host is up (0.087s latency).
Not shown: 992 filtered tcp ports (no-response), 2 filtered tcp ports (host-unreach)
PORT     STATE SERVICE    VERSION
25/tcp   open  smtp       Check Point FireWall-1 smtpd
| smtp-commands: Hello nmap.scanme.org, pleased to meet you, SIZE
|_ Commands HELO MAIL RCPT DATA RSET NOOP QUIT HELP End of HELP
80/tcp   open  http       Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
443/tcp  open  tcpwrapped
1720/tcp open  h323q931
8008/tcp open  http
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 302 Found
|     Location: https://:8015/nice%20ports%2C/Tri%6Eity.txt%2ebak
|     Connection: close
|     X-Frame-Options: SAMEORIGIN
|     X-XSS-Protection: 1; mode=block
|     X-Content-Type-Options: nosniff
|     Content-Security-Policy: frame-ancestors 'self'
|   GenericLines, HTTPOptions, RTSPRequest, SIPOptions:
|     HTTP/1.1 302 Found
|     Location: https://:8015
|     Connection: close
|     X-Frame-Options: SAMEORIGIN
|     X-XSS-Protection: 1; mode=block
|     X-Content-Type-Options: nosniff
```

| Content-Security-Policy: frame-ancestors 'self'
| Cache-Control:
| HTTP/1.1 302 Found
| Location: https://9315/
| Connection: close
| X-Frame-Options: SAMEORIGIN
| X-XSS-Protection: 1; mode=block
| X-Content-Type-Options: nosniff
|_ Content-Security-Policy: frame-ancestors 'self'
|_http-title: Did not follow redirect to https://192.15.132.41:9315/
8080/tcp open http   Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
| service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8080-TCP:V=7.93%I=7%D=2/1%Time=63DA8CDA%P=x86_64-pc-linux-gnu%r(Get
SF:Request,D5,"HTTP/1\.1\x20302\x20Found\r\nLocation:\x20https://9315/\r\
SF:nConnection:\x20close\r\nX-Frame-Options:\x20SAMEORIGIN\r\nX-XSS-Protec
SF:tion:\x201;\x20mode=block\r\nX-Content-Type-Options:\x20nosniff\r\nCont
SF:ent-Security-Policy:\x20frame-ancestors\x20'self'\r\n\r\n")%r(HTTPOptio
SF:ns,D5,"HTTP/1\.1\x20302\x20Found\r\nLocation:\x20https://9315/\r\nConne
SF:ction:\x20close\r\nX-Frame-Options:\x20SAMEORIGIN\r\nX-XSS-Protection:\
SF:x201;\x20mode=block\r\nX-Content-Type-Options:\x20nosniff\r\nContent-Se
SF:curity-Policy:\x20frame-ancestors\x20'self'\r\n\r\n")%r(RTSPRequest,D5,
SF:"HTTP/1\.1\x20302\x20Found\r\nLocation:\x20https://9315/\r\nConnection:
SF:\x20close\r\nX-Frame-Options:\x20SAMEORIGIN\r\nX-XSS-Protection:\x201;\
SF:x20mode=block\r\nX-Content-Type-Options:\x20nosniff\r\nContent-Security
SF:-Policy:\x20frame-ancestors\x20'self'\r\n\r\n")%r(FourOhFourRequest,D5,
SF:"HTTP/1\.1\x20302\x20Found\r\nLocation:\x20https://9315/\r\nConnection:
SF:\x20close\r\nX-Frame-Options:\x20SAMEORIGIN\r\nX-XSS-Protection:\x201;\
SF:x20mode=block\r\nX-Content-Type-Options:\x20nosniff\r\nContent-Security
SF:-Policy:\x20frame-ancestors\x20'self'\r\n\r\n")%r(GenericLines,D5,"HTTP
SF:/1\.1\x20302\x20Found\r\nLocation:\x20https://9315/\r\nConnection:\x20c
SF:lose\r\nX-Frame-Options:\x20SAMEORIGIN\r\nX-XSS-Protection:\x201;\x20mo
SF:de=block\r\nX-Content-Type-Options:\x20nosniff\r\nContent-Security-Poli
SF:cy:\x20frame-ancestors\x20'self'\r\n\r\n")%r(Help,D5,"HTTP/1\.1\x20302
SF:\x20Found\r\nLocation:\x20https://9315/\r\nConnection:\x20close\r\nX-Fra
SF:me-Options:\x20SAMEORIGIN\r\nX-XSS-Protection:\x201;\x20mode=block\r\nX
SF:-Content-Type-Options:\x20nosniff\r\nContent-Security-Policy:\x20frame-
SF:ancestors\x20'self'\r\n\r\n")%r(SSLSessionReq,D5,"HTTP/1\.1\x20302\x20F
SF:ound\r\nLocation:\x20https://9315/\r\nConnection:\x20close\r\nX-Frame-O
SF:ptions:\x20SAMEORIGIN\r\nX-XSS-Protection:\x201;\x20mode=block\r\nX-Con
SF:tent-Type-Options:\x20nosniff\r\nContent-Security-Policy:\x20frame-ance
SF:stors\x20'self'\r\n\r\n");

```
SF:e;\r\n\r\n")%r(RTSPRequest,D2,"HTTP/1\.1\x20302\x20Found\r\nLocation:
SF:\x20https://:8015\r\nConnection:\x20close\r\nX-Frame-Options:\x20SAMEOR
SF:IGIN\r\nX-XSS-Protection:\x201;\x20mode=block\r\nX-Content-Type-Options
SF::\x20nosniff\r\nContent-Security-Policy:\x20frame-ancestors\x20'self'\r
SF:\n\r\n")%r(SIPOptions,D2,"HTTP/1\.1\x20302\x20Found\r\nLocation:\x20htt
SF:ps://:8015\r\nConnection:\x20close\r\nX-Frame-Options:\x20SAMEORIGIN\r
SF:\nX-XSS-Protection:\x201;\x20mode=block\r\nX-Content-Type-Options:\x20no
SF:sniff\r\nContent-Security-Policy:\x20frame-ancestors\x20'self'\r\n\r\n"
SF:);
Service Info: Device: firewall

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 283.20 seconds

┌──(hmstudent㉿hmstudent)-[~]
└─$
```

ANEXO J

UCACUR_ISTA

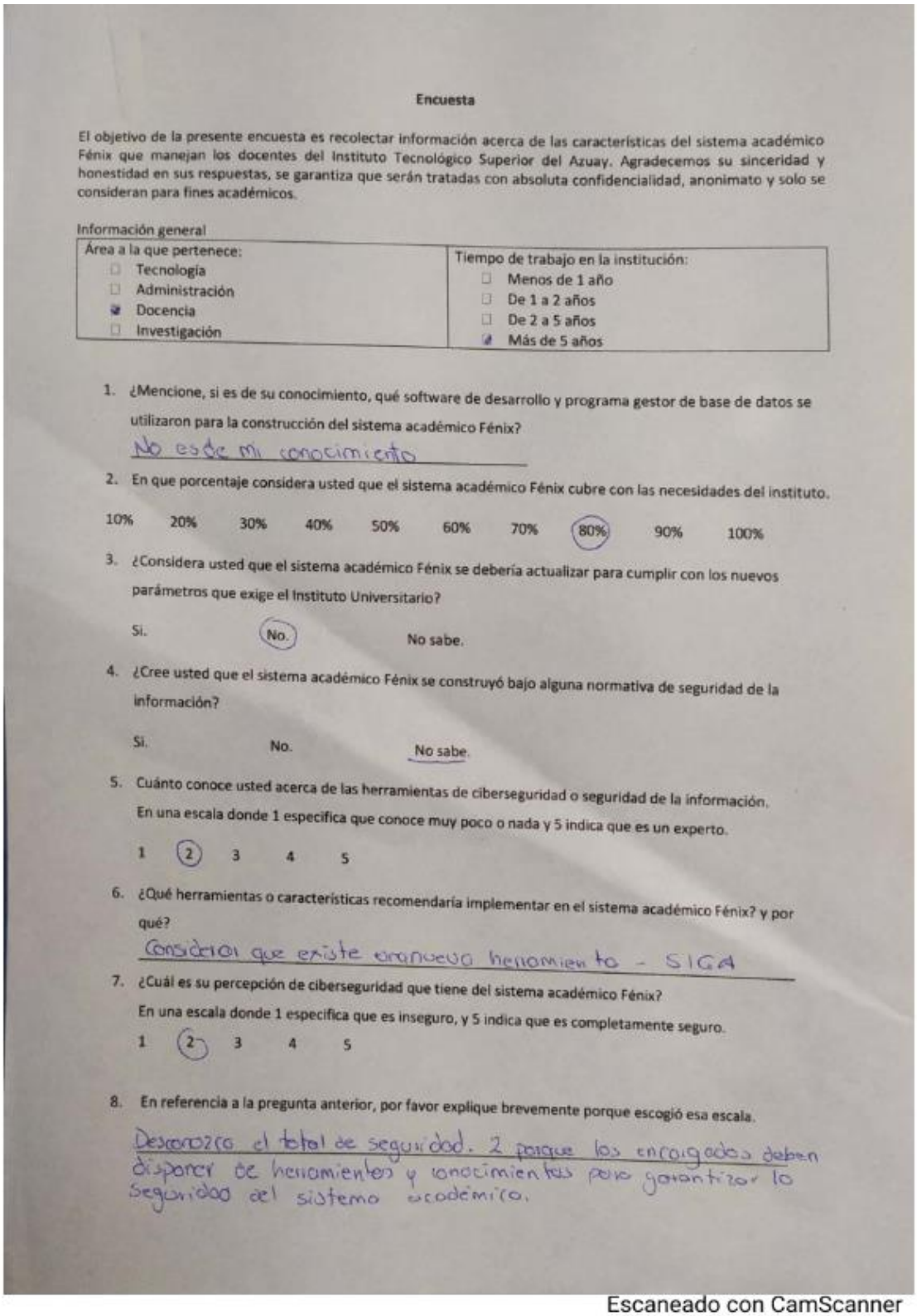
Report generated by Nessus™ Tue, 31 Jan 2023 19:03:25 EST

Vulnerabilities Total: 1

SEVERITY	CVSS V3.0	PLUGIN	NAME
INFO		19506	Nessus Scan Information

* indicates the v3.0 score was not available; the v2.0 score is shown

ANEXO K



Encuesta

El objetivo de la presente encuesta es recolectar información acerca de las características del sistema académico Fénix que manejan los docentes del Instituto Tecnológico Superior del Azuay. Agradecemos su sinceridad y honestidad en sus respuestas, se garantiza que serán tratadas con absoluta confidencialidad, anonimato y solo se consideran para fines académicos.

Información general

Área a la que pertenece:	Tiempo de trabajo en la institución:
☐ Tecnología	☐ Menos de 1 año
☐ Administración	☐ De 1 a 2 años
☑ Docencia	☐ De 2 a 5 años
☐ Investigación	☑ Más de 5 años

1. ¿Mencione, si es de su conocimiento, qué software de desarrollo y programa gestor de base de datos se utilizaron para la construcción del sistema académico Fénix?

   No este mi conocimiento

2. En que porcentaje considera usted que el sistema académico Fénix cubre con las necesidades del instituto.

   10% 20% 30% 40% 50% 60% 70% (80%) 90% 100%

3. ¿Considera usted que el sistema académico Fénix se debería actualizar para cumplir con los nuevos parámetros que exige el Instituto Universitario?

   Si. (No.) No sabe.

4. ¿Cree usted que el sistema académico Fénix se construyó bajo alguna normativa de seguridad de la información?

   Si. No. No sabe.

5. Cuánto conoce usted acerca de las herramientas de ciberseguridad o seguridad de la información.

   En una escala donde 1 especifica que conoce muy poco o nada y 5 indica que es un experto.

   1 (2) 3 4 5

6. ¿Qué herramientas o características recomendaría implementar en el sistema académico Fénix? y por qué?

   Considero que existe otra nueva herramienta - SIGA

7. ¿Cuál es su percepción de ciberseguridad que tiene del sistema académico Fénix?

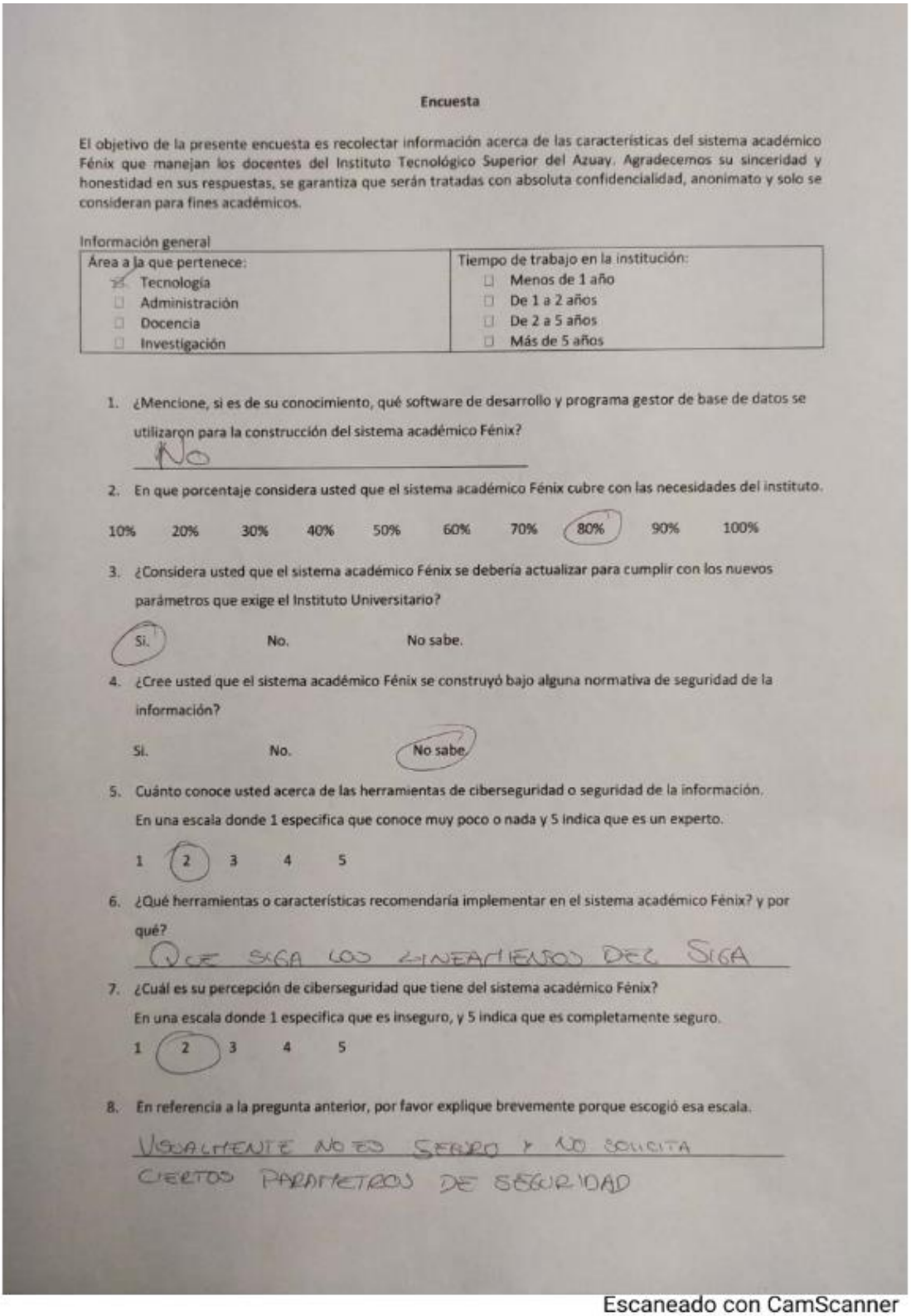
   En una escala donde 1 especifica que es inseguro, y 5 indica que es completamente seguro.

   1 (2) 3 4 5

8. En referencia a la pregunta anterior, por favor explique brevemente porque escogió esa escala.

   Desconozco el total de seguridad. 2 porque los encargados deben disponer de herramientas y conocimientos para garantizar la seguridad del sistema académico.

Escaneado con CamScanner



Encuesta

El objetivo de la presente encuesta es recolectar información acerca de las características del sistema académico Fénix que manejan los docentes del Instituto Tecnológico Superior del Azuay. Agradecemos su sinceridad y honestidad en sus respuestas, se garantiza que serán tratadas con absoluta confidencialidad, anonimato y solo se consideran para fines académicos.

Información general

Área a la que pertenece:	Tiempo de trabajo en la institución:
☒ Tecnología	☐ Menos de 1 año
☐ Administración	☐ De 1 a 2 años
☐ Docencia	☐ De 2 a 5 años
☐ Investigación	☐ Más de 5 años

1. ¿Mencione, si es de su conocimiento, qué software de desarrollo y programa gestor de base de datos se utilizaron para la construcción del sistema académico Fénix?

   No

2. En que porcentaje considera usted que el sistema académico Fénix cubre con las necesidades del instituto.

   10% 20% 30% 40% 50% 60% 70% (80%) 90% 100%

3. ¿Considera usted que el sistema académico Fénix se debería actualizar para cumplir con los nuevos parámetros que exige el Instituto Universitario?

   (Si.) No. No sabe.

4. ¿Cree usted que el sistema académico Fénix se construyó bajo alguna normativa de seguridad de la información?

   Si. No. (No sabe.)

5. Cuánto conoce usted acerca de las herramientas de ciberseguridad o seguridad de la información.
   En una escala donde 1 especifica que conoce muy poco o nada y 5 indica que es un experto.

   1 (2) 3 4 5

6. ¿Qué herramientas o características recomendaría implementar en el sistema académico Fénix? y por qué?

   QUE SIGA LOS LINEAMIENTOS DEL SIGA

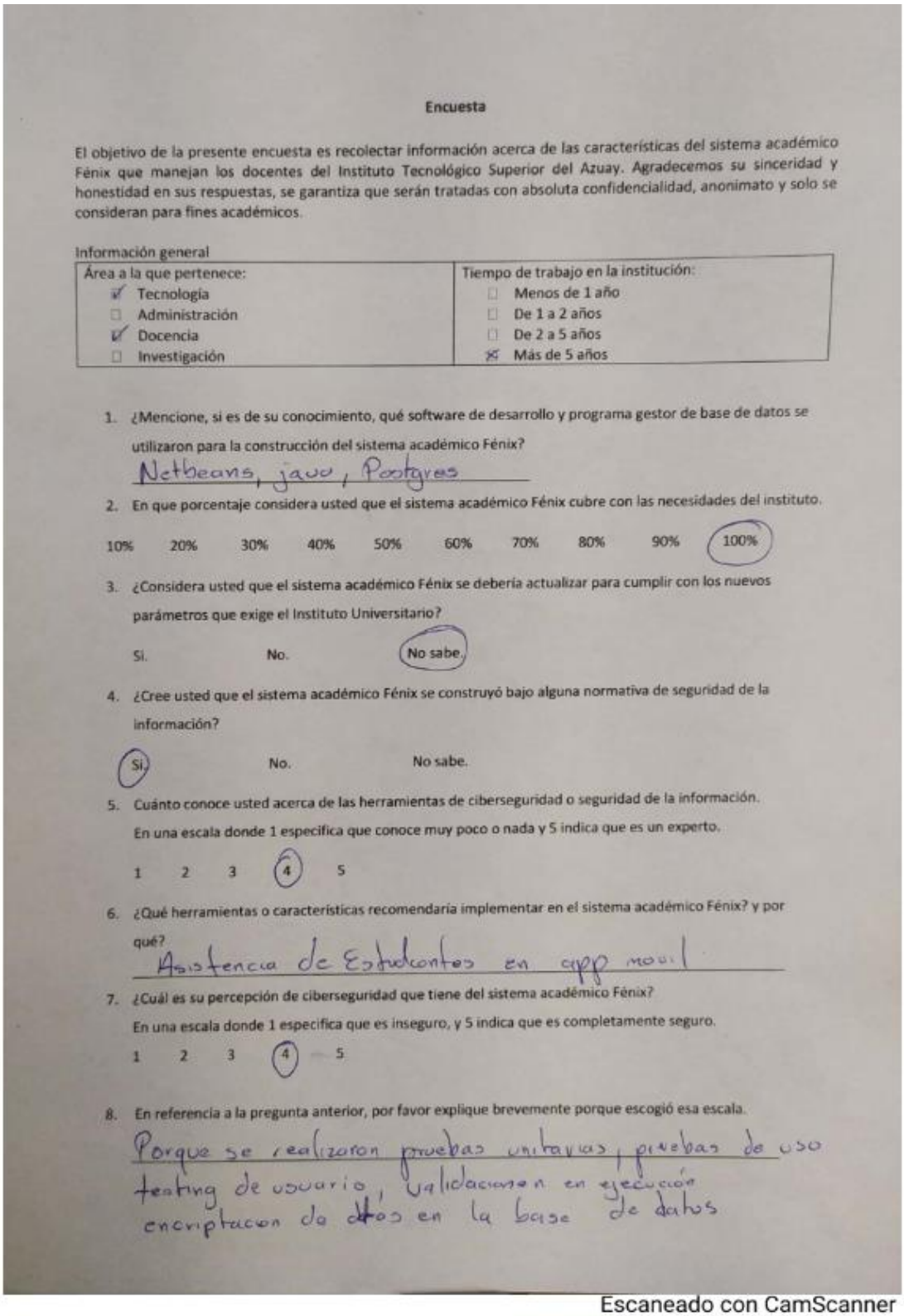
7. ¿Cuál es su percepción de ciberseguridad que tiene del sistema académico Fénix?
   En una escala donde 1 especifica que es inseguro, y 5 indica que es completamente seguro.

   1 (2) 3 4 5

8. En referencia a la pregunta anterior, por favor explique brevemente porque escogió esa escala.

   VISUALMENTE NO ES SEGURO Y NO SOLICITA CIERTOS PARAMETROS DE SEGURIDAD

Escaneado con CamScanner



Encuesta

El objetivo de la presente encuesta es recolectar información acerca de las características del sistema académico Fénix que manejan los docentes del Instituto Tecnológico Superior del Azuay. Agradecemos su sinceridad y honestidad en sus respuestas, se garantiza que serán tratadas con absoluta confidencialidad, anonimato y solo se consideran para fines académicos.

Información general

Área a la que pertenece:	Tiempo de trabajo en la institución:
☑ Tecnología	☐ Menos de 1 año
☐ Administración	☐ De 1 a 2 años
☑ Docencia	☐ De 2 a 5 años
☐ Investigación	☒ Más de 5 años

1. ¿Mencione, si es de su conocimiento, qué software de desarrollo y programa gestor de base de datos se utilizaron para la construcción del sistema académico Fénix?

   Netbeans, java, Postgres

2. En que porcentaje considera usted que el sistema académico Fénix cubre con las necesidades del instituto.

   10% 20% 30% 40% 50% 60% 70% 80% 90% (100%)

3. ¿Considera usted que el sistema académico Fénix se debería actualizar para cumplir con los nuevos parámetros que exige el Instituto Universitario?

   Si. No. (No sabe.)

4. ¿Cree usted que el sistema académico Fénix se construyó bajo alguna normativa de seguridad de la información?

   (Si.) No. No sabe.

5. Cuánto conoce usted acerca de las herramientas de ciberseguridad o seguridad de la información.
   En una escala donde 1 especifica que conoce muy poco o nada y 5 indica que es un experto.

   1 2 3 (4) 5

6. ¿Qué herramientas o características recomendaría implementar en el sistema académico Fénix? y por qué?

   Asistencia de Estudiantes en app movil

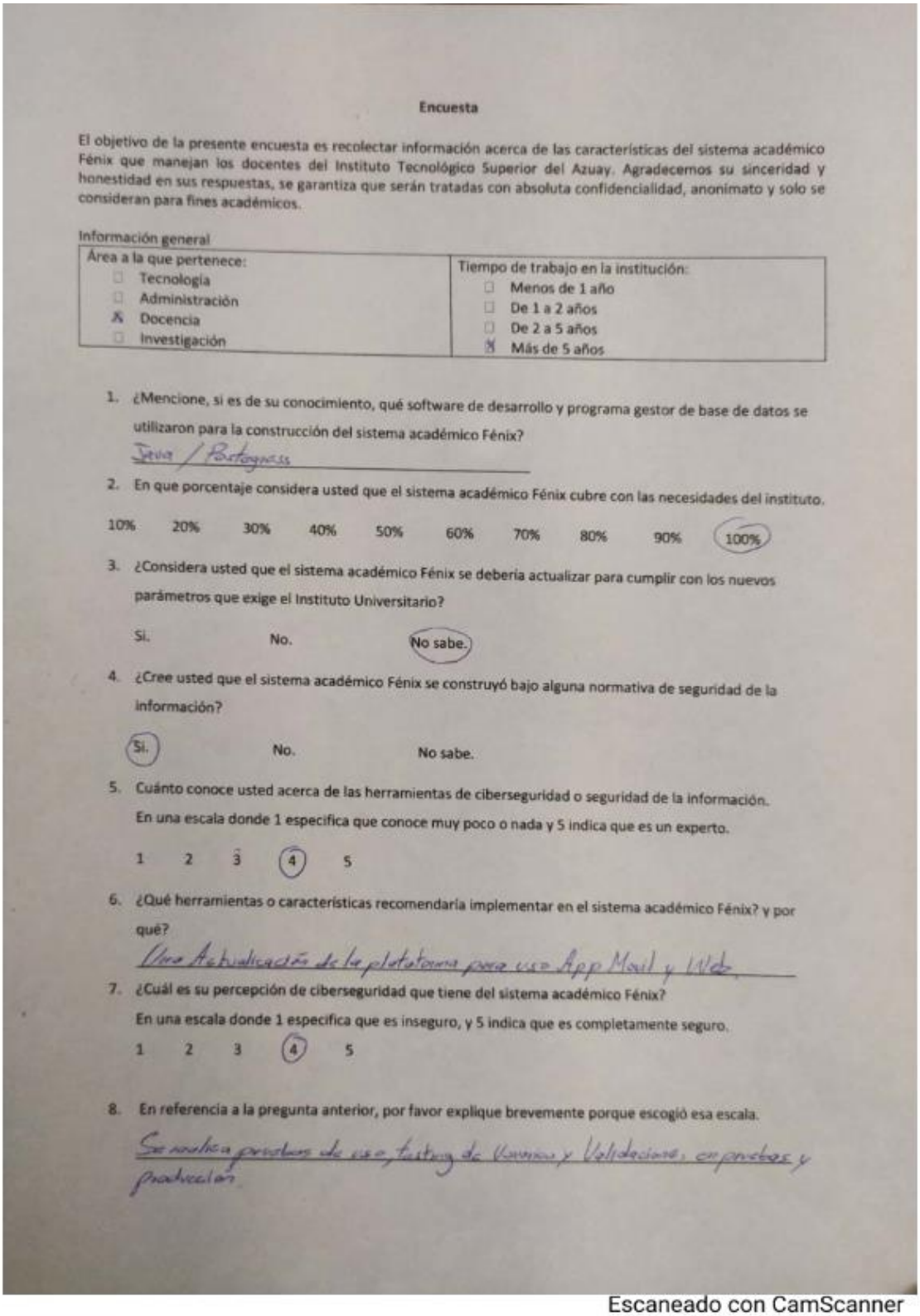
7. ¿Cuál es su percepción de ciberseguridad que tiene del sistema académico Fénix?
   En una escala donde 1 especifica que es inseguro, y 5 indica que es completamente seguro.

   1 2 3 (4) 5

8. En referencia a la pregunta anterior, por favor explique brevemente porque escogió esa escala.

   Porque se realizaron pruebas unitarias, pruebas de uso testing de usuario, validaciones en ejecución encriptacion de datos en la base de datos

Escaneado con CamScanner



Encuesta

El objetivo de la presente encuesta es recolectar información acerca de las características del sistema académico Fénix que manejan los docentes del Instituto Tecnológico Superior del Azuay. Agradecemos su sinceridad y honestidad en sus respuestas, se garantiza que serán tratadas con absoluta confidencialidad, anonimato y solo se consideran para fines académicos.

Información general

Área a la que pertenece:	Tiempo de trabajo en la institución:
☐ Tecnología	☐ Menos de 1 año
☐ Administración	☐ De 1 a 2 años
☒ Docencia	☐ De 2 a 5 años
☐ Investigación	☒ Más de 5 años

1. ¿Mencione, si es de su conocimiento, qué software de desarrollo y programa gestor de base de datos se utilizaron para la construcción del sistema académico Fénix?

   Java / Portogress

2. En que porcentaje considera usted que el sistema académico Fénix cubre con las necesidades del instituto.

   10% 20% 30% 40% 50% 60% 70% 80% 90% (100%)

3. ¿Considera usted que el sistema académico Fénix se debería actualizar para cumplir con los nuevos parámetros que exige el Instituto Universitario?

   Si. No. (No sabe.)

4. ¿Cree usted que el sistema académico Fénix se construyó bajo alguna normativa de seguridad de la información?

   (Si.) No. No sabe.

5. Cuánto conoce usted acerca de las herramientas de ciberseguridad o seguridad de la información.
   En una escala donde 1 especifica que conoce muy poco o nada y 5 indica que es un experto.

   1 2 3 (4) 5

6. ¿Qué herramientas o características recomendaría implementar en el sistema académico Fénix? y por qué?

   Una Actualización de la plataforma para uso App Movil y Web.

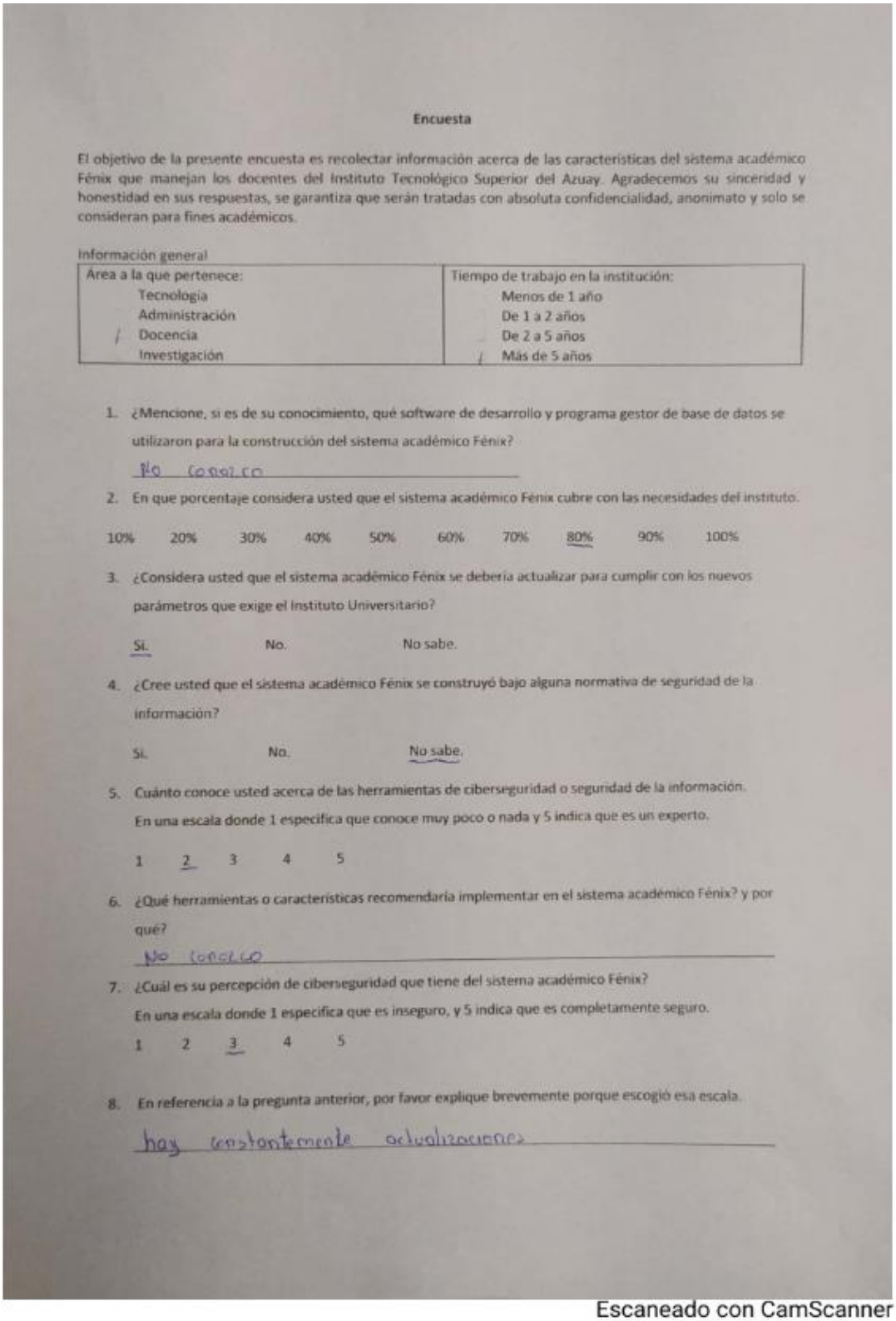
7. ¿Cuál es su percepción de ciberseguridad que tiene del sistema académico Fénix?
   En una escala donde 1 especifica que es inseguro, y 5 indica que es completamente seguro.

   1 2 3 (4) 5

8. En referencia a la pregunta anterior, por favor explique brevemente porque escogió esa escala.

   Se realiza pruebas de uso, testing de Usuario y Validaciones, en pruebas y producción.

Escaneado con CamScanner



Encuesta

El objetivo de la presente encuesta es recolectar información acerca de las características del sistema académico Fénix que manejan los docentes del Instituto Tecnológico Superior del Azuay. Agradecemos su sinceridad y honestidad en sus respuestas, se garantiza que serán tratadas con absoluta confidencialidad, anonimato y solo se consideran para fines académicos.

Información general

Area a la que pertenece:	Tiempo de trabajo en la institución:
Tecnología	Menos de 1 año
Administración	De 1 a 2 años
/ Docencia	De 2 a 5 años
Investigación	/ Más de 5 años

1. ¿Mencione, si es de su conocimiento, qué software de desarrollo y programa gestor de base de datos se utilizaron para la construcción del sistema académico Fénix?

   No conozco

2. En que porcentaje considera usted que el sistema académico Fénix cubre con las necesidades del instituto.

   10% 20% 30% 40% 50% 60% 70% 80% 90% 100%

3. ¿Considera usted que el sistema académico Fénix se debería actualizar para cumplir con los nuevos parámetros que exige el Instituto Universitario?

   Si. No. No sabe.

4. ¿Cree usted que el sistema académico Fénix se construyó bajo alguna normativa de seguridad de la información?

   Si. No. No sabe.

5. Cuánto conoce usted acerca de las herramientas de ciberseguridad o seguridad de la información.
   En una escala donde 1 especifica que conoce muy poco o nada y 5 indica que es un experto.

   1 2 3 4 5

6. ¿Qué herramientas o características recomendaría implementar en el sistema académico Fénix? y por qué?

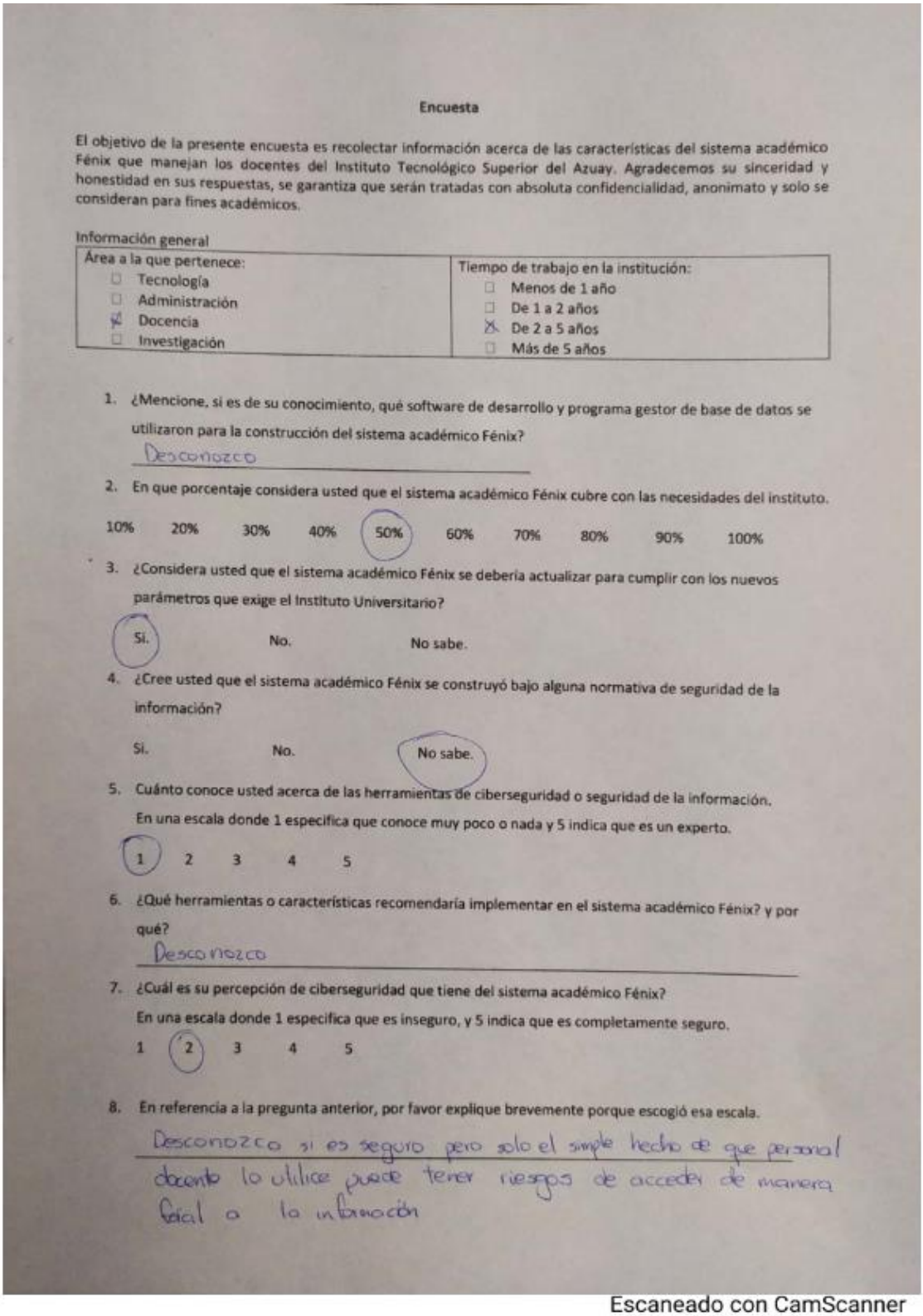
   No conozco

7. ¿Cuál es su percepción de ciberseguridad que tiene del sistema académico Fénix?
   En una escala donde 1 especifica que es inseguro, y 5 indica que es completamente seguro.

   1 2 3 4 5

8. En referencia a la pregunta anterior, por favor explique brevemente porque escogió esa escala.

   hay constantemente actualizaciones



Encuesta

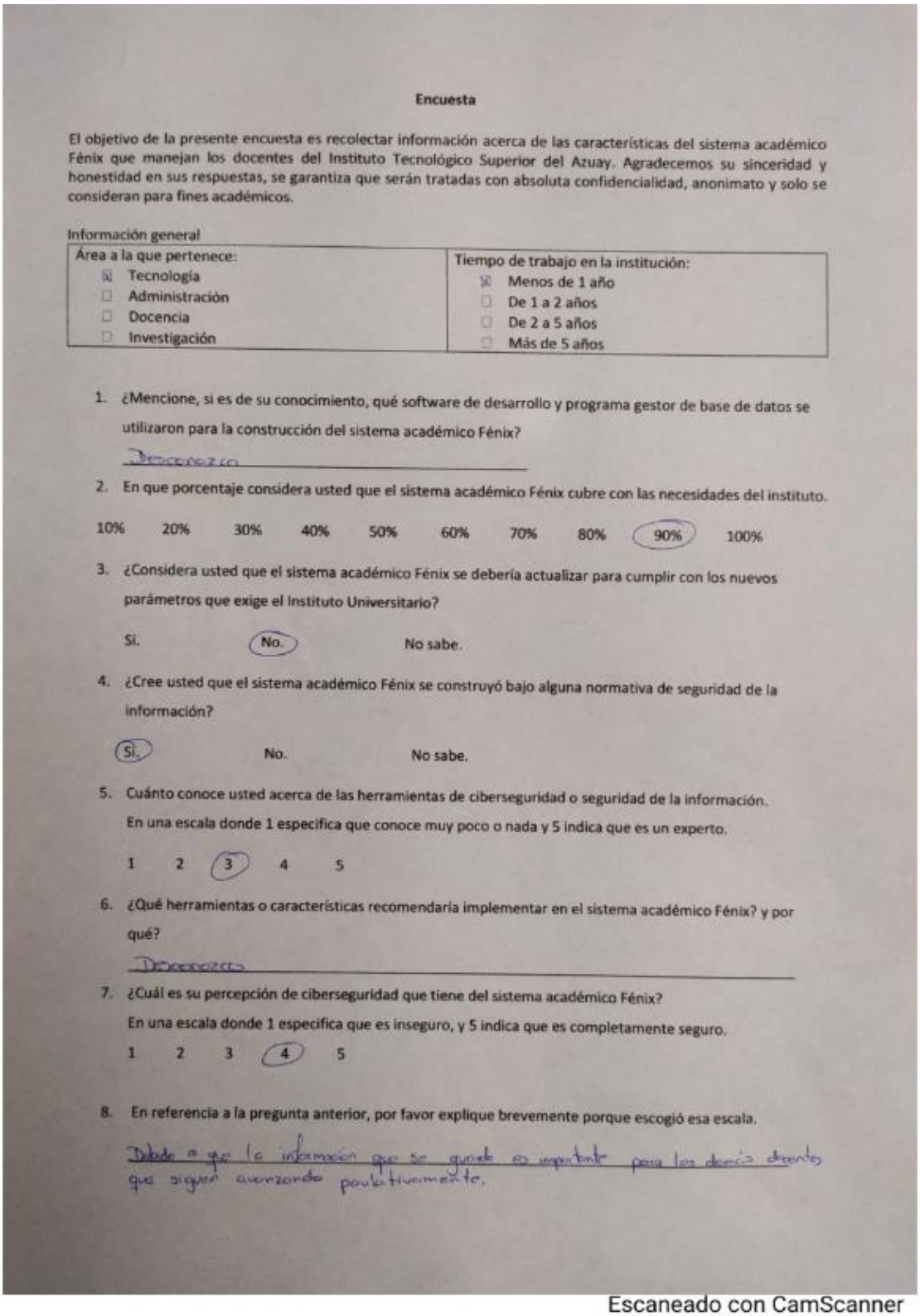
El objetivo de la presente encuesta es recolectar información acerca de las características del sistema académico Fénix que manejan los docentes del Instituto Tecnológico Superior del Azuay. Agradecemos su sinceridad y honestidad en sus respuestas, se garantiza que serán tratadas con absoluta confidencialidad, anonimato y solo se consideran para fines académicos.

Información general

Área a la que pertenece:	Tiempo de trabajo en la institución:
☐ Tecnología	☐ Menos de 1 año
☐ Administración	☐ De 1 a 2 años
☑ Docencia	☒ De 2 a 5 años
☐ Investigación	☐ Más de 5 años

1. ¿Mencione, si es de su conocimiento, qué software de desarrollo y programa gestor de base de datos se utilizaron para la construcción del sistema académico Fénix?
   Desconozco
2. En que porcentaje considera usted que el sistema académico Fénix cubre con las necesidades del instituto.
   10% 20% 30% 40% (50%) 60% 70% 80% 90% 100%
3. ¿Considera usted que el sistema académico Fénix se debería actualizar para cumplir con los nuevos parámetros que exige el Instituto Universitario?
   (Si.) No. No sabe.
4. ¿Cree usted que el sistema académico Fénix se construyó bajo alguna normativa de seguridad de la información?
   Si. No. (No sabe.)
5. Cuánto conoce usted acerca de las herramientas de ciberseguridad o seguridad de la información.
   En una escala donde 1 especifica que conoce muy poco o nada y 5 indica que es un experto.
   (1) 2 3 4 5
6. ¿Qué herramientas o características recomendaría implementar en el sistema académico Fénix? y por qué?
   Desconozco
7. ¿Cuál es su percepción de ciberseguridad que tiene del sistema académico Fénix?
   En una escala donde 1 especifica que es inseguro, y 5 indica que es completamente seguro.
   1 (2) 3 4 5
8. En referencia a la pregunta anterior, por favor explique brevemente porque escogió esa escala.
   Desconozco si es seguro pero solo el simple hecho de que personal docente lo utilice puede tener riesgos de acceder de manera facil a la información

Escaneado con CamScanner



Encuesta

El objetivo de la presente encuesta es recolectar información acerca de las características del sistema académico Fénix que manejan los docentes del Instituto Tecnológico Superior del Azuay. Agradecemos su sinceridad y honestidad en sus respuestas, se garantiza que serán tratadas con absoluta confidencialidad, anonimato y solo se consideran para fines académicos.

Información general

Área a la que pertenece:	Tiempo de trabajo en la institución:
☒ Tecnología	☒ Menos de 1 año
☐ Administración	☐ De 1 a 2 años
☐ Docencia	☐ De 2 a 5 años
☐ Investigación	☐ Más de 5 años

1. ¿Mencione, si es de su conocimiento, qué software de desarrollo y programa gestor de base de datos se utilizaron para la construcción del sistema académico Fénix?

   Desconozco

2. En que porcentaje considera usted que el sistema académico Fénix cubre con las necesidades del instituto.

   10% 20% 30% 40% 50% 60% 70% 80% (90%) 100%

3. ¿Considera usted que el sistema académico Fénix se debería actualizar para cumplir con los nuevos parámetros que exige el Instituto Universitario?

   Si. (No.) No sabe.

4. ¿Cree usted que el sistema académico Fénix se construyó bajo alguna normativa de seguridad de la información?

   (Si.) No. No sabe.

5. Cuánto conoce usted acerca de las herramientas de ciberseguridad o seguridad de la información.
   En una escala donde 1 especifica que conoce muy poco o nada y 5 indica que es un experto.

   1 2 (3) 4 5

6. ¿Qué herramientas o características recomendaría implementar en el sistema académico Fénix? y por qué?

   Desconozco

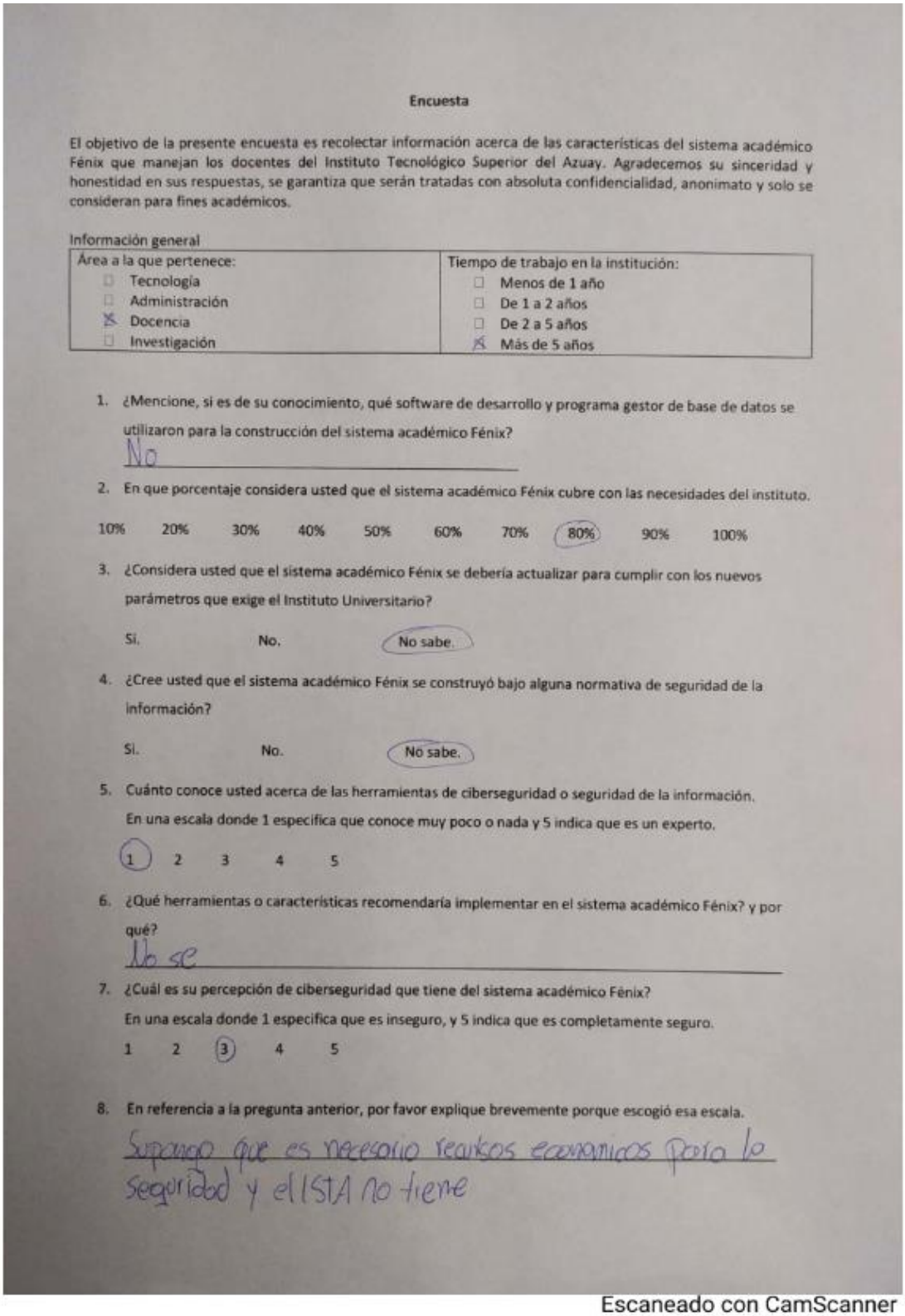
7. ¿Cuál es su percepción de ciberseguridad que tiene del sistema académico Fénix?
   En una escala donde 1 especifica que es inseguro, y 5 indica que es completamente seguro.

   1 2 3 (4) 5

8. En referencia a la pregunta anterior, por favor explique brevemente porque escogió esa escala.

   Debido a que la información que se guarda es importante para los docentes que siguen avanzando positivamente.

Escaneado con CamScanner



Encuesta

El objetivo de la presente encuesta es recolectar información acerca de las características del sistema académico Fénix que manejan los docentes del Instituto Tecnológico Superior del Azuay. Agradecemos su sinceridad y honestidad en sus respuestas, se garantiza que serán tratadas con absoluta confidencialidad, anonimato y solo se consideran para fines académicos.

Información general

Área a la que pertenece:	Tiempo de trabajo en la institución:
☐ Tecnología	☐ Menos de 1 año
☐ Administración	☐ De 1 a 2 años
☒ Docencia	☐ De 2 a 5 años
☐ Investigación	☒ Más de 5 años

1. ¿Mencione, si es de su conocimiento, qué software de desarrollo y programa gestor de base de datos se utilizaron para la construcción del sistema académico Fénix?

   No

2. En que porcentaje considera usted que el sistema académico Fénix cubre con las necesidades del instituto.

   10% 20% 30% 40% 50% 60% 70% (80%) 90% 100%

3. ¿Considera usted que el sistema académico Fénix se debería actualizar para cumplir con los nuevos parámetros que exige el Instituto Universitario?

   Si. No. (No sabe.)

4. ¿Cree usted que el sistema académico Fénix se construyó bajo alguna normativa de seguridad de la información?

   Si. No. (No sabe.)

5. Cuánto conoce usted acerca de las herramientas de ciberseguridad o seguridad de la información.

   En una escala donde 1 especifica que conoce muy poco o nada y 5 indica que es un experto.

   (1) 2 3 4 5

6. ¿Qué herramientas o características recomendaría implementar en el sistema académico Fénix? y por qué?

   No se

7. ¿Cuál es su percepción de ciberseguridad que tiene del sistema académico Fénix?

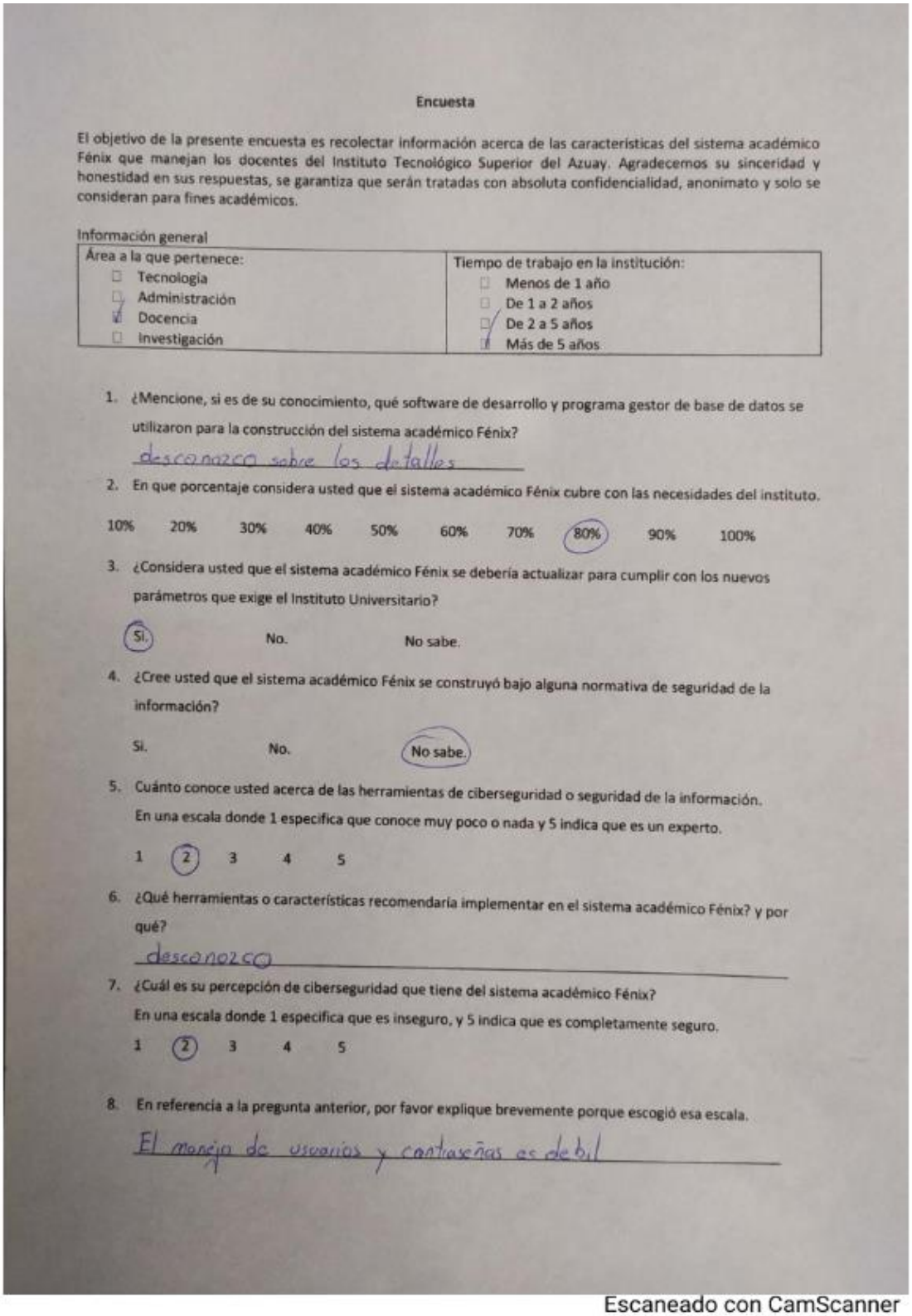
   En una escala donde 1 especifica que es inseguro, y 5 indica que es completamente seguro.

   1 2 (3) 4 5

8. En referencia a la pregunta anterior, por favor explique brevemente porque escogió esa escala.

   Supongo que es necesario recursos económicos para la seguridad y el ISTA no tiene

Escaneado con CamScanner



Encuesta

El objetivo de la presente encuesta es recolectar información acerca de las características del sistema académico Fénix que manejan los docentes del Instituto Tecnológico Superior del Azuay. Agradecemos su sinceridad y honestidad en sus respuestas, se garantiza que serán tratadas con absoluta confidencialidad, anonimato y solo se consideran para fines académicos.

Información general

Área a la que pertenece:	Tiempo de trabajo en la institución:
☐ Tecnología	☐ Menos de 1 año
☐ Administración	☐ De 1 a 2 años
☑ Docencia	☐ De 2 a 5 años
☐ Investigación	☑ Más de 5 años

1. ¿Mencione, si es de su conocimiento, qué software de desarrollo y programa gestor de base de datos se utilizaron para la construcción del sistema académico Fénix?

   desconozco sobre los detalles

2. En que porcentaje considera usted que el sistema académico Fénix cubre con las necesidades del instituto.

   10% 20% 30% 40% 50% 60% 70% (80%) 90% 100%

3. ¿Considera usted que el sistema académico Fénix se debería actualizar para cumplir con los nuevos parámetros que exige el Instituto Universitario?

   (Si.) No. No sabe.

4. ¿Cree usted que el sistema académico Fénix se construyó bajo alguna normativa de seguridad de la información?

   Si. No. (No sabe.)

5. Cuánto conoce usted acerca de las herramientas de ciberseguridad o seguridad de la información.
   En una escala donde 1 especifica que conoce muy poco o nada y 5 indica que es un experto.

   1 (2) 3 4 5

6. ¿Qué herramientas o características recomendaría implementar en el sistema académico Fénix? y por qué?

   desconozco

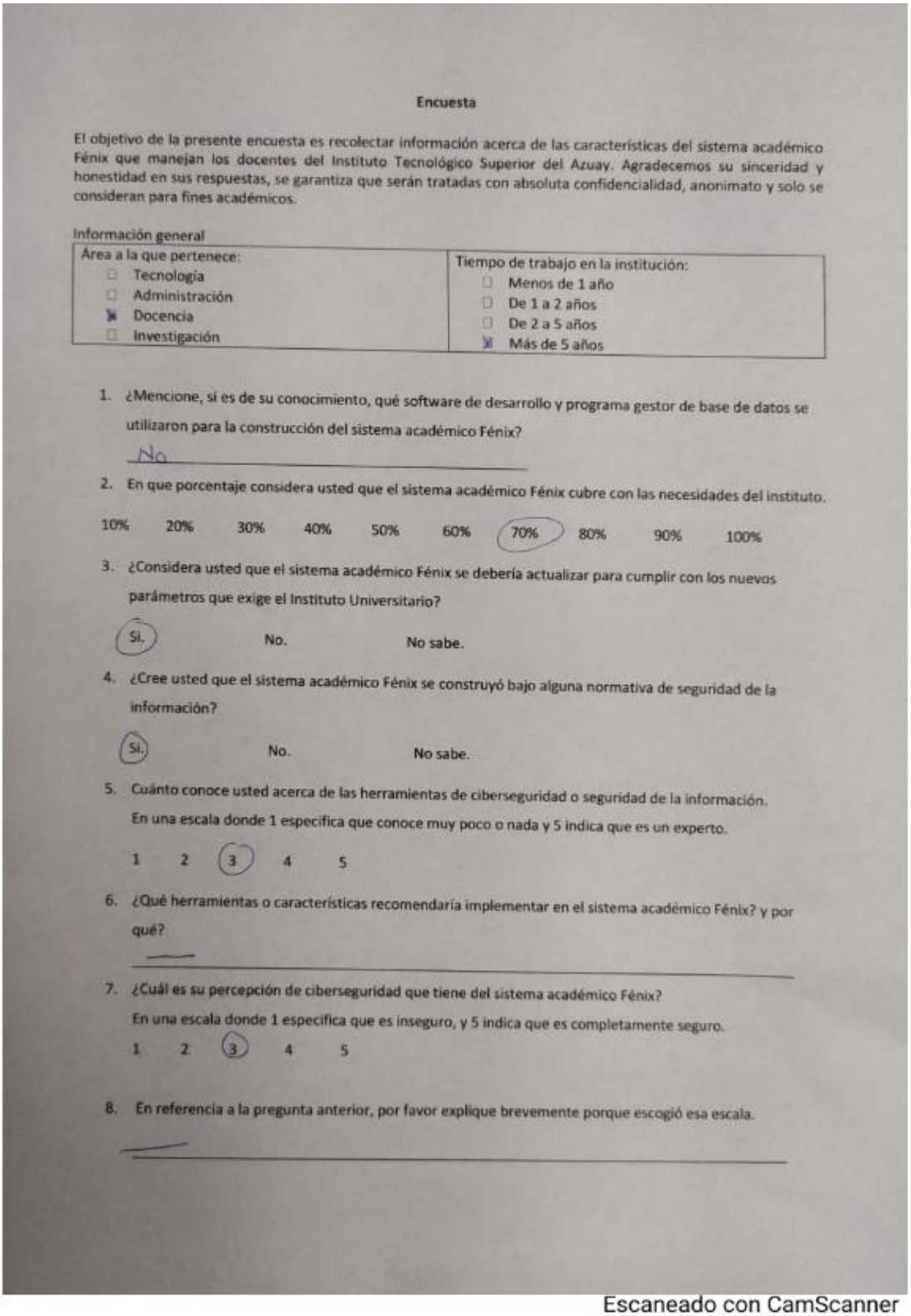
7. ¿Cuál es su percepción de ciberseguridad que tiene del sistema académico Fénix?
   En una escala donde 1 especifica que es inseguro, y 5 indica que es completamente seguro.

   1 (2) 3 4 5

8. En referencia a la pregunta anterior, por favor explique brevemente porque escogió esa escala.

   El manejo de usuarios y contraseñas es debil

Escaneado con CamScanner



Encuesta

El objetivo de la presente encuesta es recolectar información acerca de las características del sistema académico Fénix que manejan los docentes del Instituto Tecnológico Superior del Azuay. Agradecemos su sinceridad y honestidad en sus respuestas, se garantiza que serán tratadas con absoluta confidencialidad, anonimato y solo se consideran para fines académicos.

Información general

Área a la que pertenece:	Tiempo de trabajo en la institución:
☐ Tecnología	☐ Menos de 1 año
☐ Administración	☐ De 1 a 2 años
☒ Docencia	☐ De 2 a 5 años
☐ Investigación	☒ Más de 5 años

1. ¿Mencione, si es de su conocimiento, qué software de desarrollo y programa gestor de base de datos se utilizaron para la construcción del sistema académico Fénix?

   No

2. En que porcentaje considera usted que el sistema académico Fénix cubre con las necesidades del instituto.

   10% 20% 30% 40% 50% 60% (70%) 80% 90% 100%

3. ¿Considera usted que el sistema académico Fénix se debería actualizar para cumplir con los nuevos parámetros que exige el Instituto Universitario?

   (Si.) No. No sabe.

4. ¿Cree usted que el sistema académico Fénix se construyó bajo alguna normativa de seguridad de la información?

   (Si.) No. No sabe.

5. Cuánto conoce usted acerca de las herramientas de ciberseguridad o seguridad de la información.
   En una escala donde 1 especifica que conoce muy poco o nada y 5 indica que es un experto.

   1 2 (3) 4 5

6. ¿Qué herramientas o características recomendaría implementar en el sistema académico Fénix? y por qué?

   —

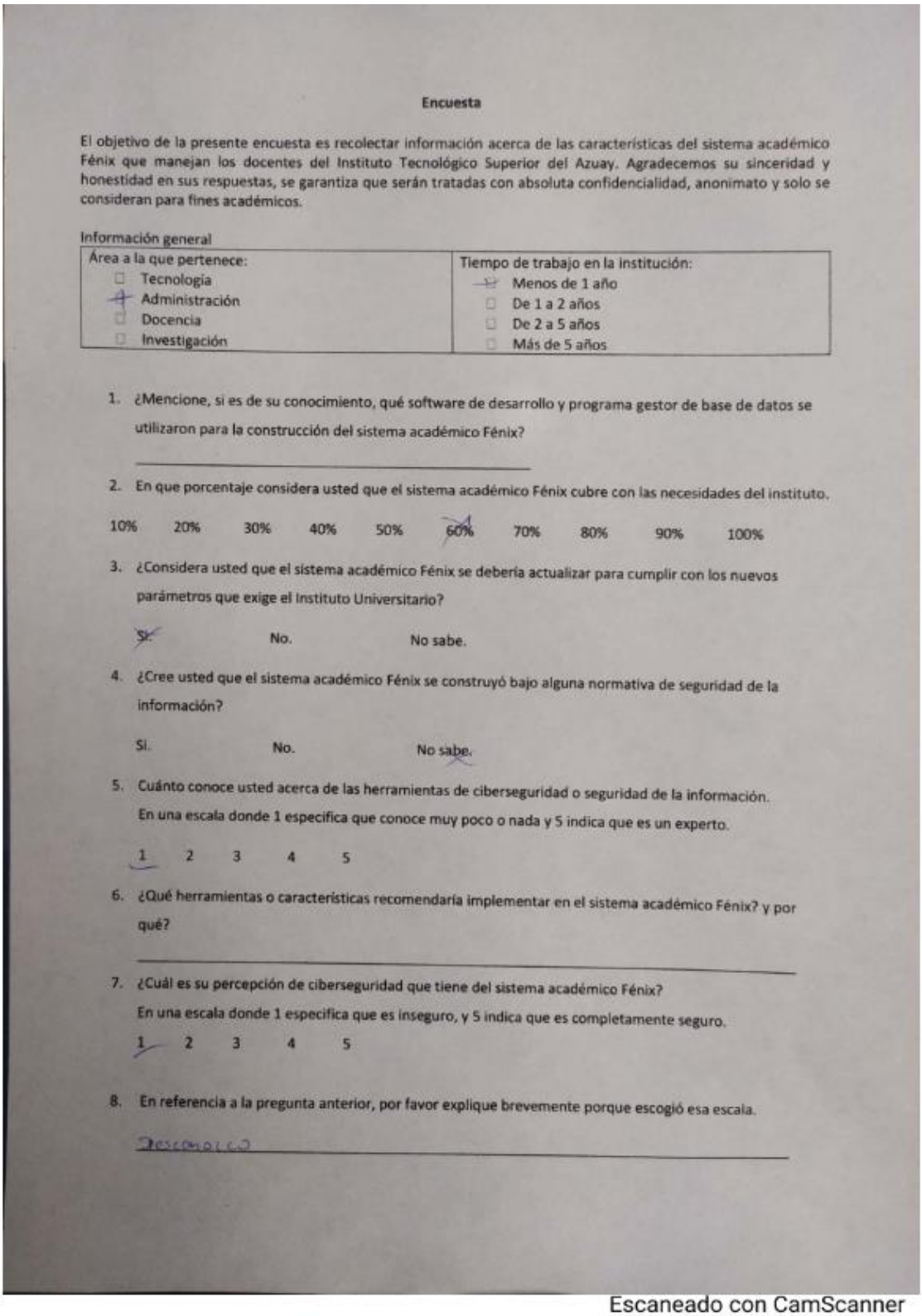
7. ¿Cuál es su percepción de ciberseguridad que tiene del sistema académico Fénix?
   En una escala donde 1 especifica que es inseguro, y 5 indica que es completamente seguro.

   1 2 (3) 4 5

8. En referencia a la pregunta anterior, por favor explique brevemente porque escogió esa escala.

   —

Escaneado con CamScanner



Encuesta

El objetivo de la presente encuesta es recolectar información acerca de las características del sistema académico Fénix que manejan los docentes del Instituto Tecnológico Superior del Azuay. Agradecemos su sinceridad y honestidad en sus respuestas, se garantiza que serán tratadas con absoluta confidencialidad, anonimato y solo se consideran para fines académicos.

Información general

Área a la que pertenece:	Tiempo de trabajo en la institución:
☐ Tecnología	☒ Menos de 1 año
☒ Administración	☐ De 1 a 2 años
☐ Docencia	☐ De 2 a 5 años
☐ Investigación	☐ Más de 5 años

1. ¿Mencione, si es de su conocimiento, qué software de desarrollo y programa gestor de base de datos se utilizaron para la construcción del sistema académico Fénix?

   _____

2. En que porcentaje considera usted que el sistema académico Fénix cubre con las necesidades del instituto.

   10% 20% 30% 40% 50% 60% 70% 80% 90% 100%

3. ¿Considera usted que el sistema académico Fénix se debería actualizar para cumplir con los nuevos parámetros que exige el Instituto Universitario?

   Si. No. No sabe.

4. ¿Cree usted que el sistema académico Fénix se construyó bajo alguna normativa de seguridad de la información?

   Si. No. No sabe.

5. Cuánto conoce usted acerca de las herramientas de ciberseguridad o seguridad de la información.
   En una escala donde 1 especifica que conoce muy poco o nada y 5 indica que es un experto.

   1 2 3 4 5

6. ¿Qué herramientas o características recomendaría implementar en el sistema académico Fénix? y por qué?

   _____

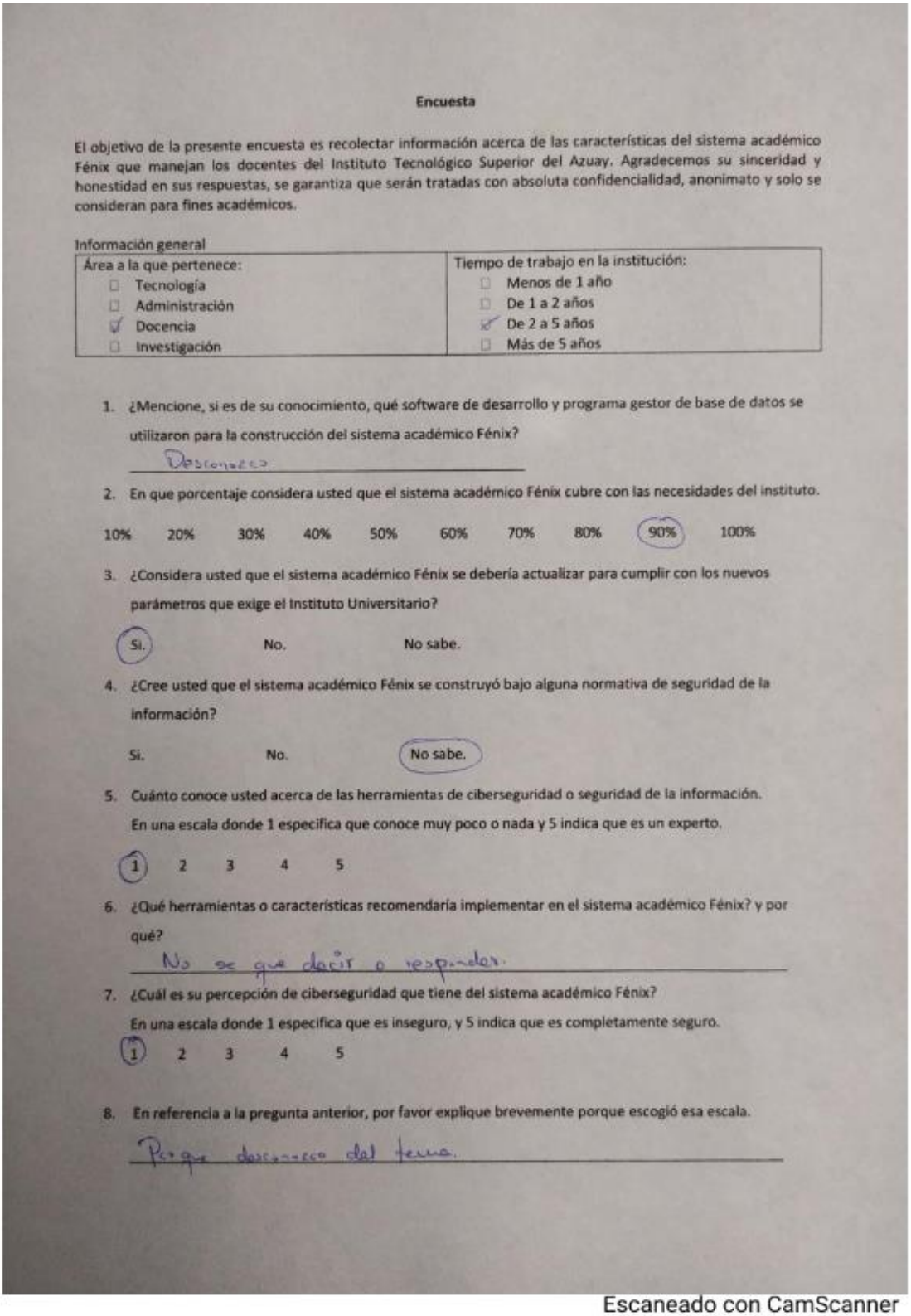
7. ¿Cuál es su percepción de ciberseguridad que tiene del sistema académico Fénix?
   En una escala donde 1 especifica que es inseguro, y 5 indica que es completamente seguro.

   1 2 3 4 5

8. En referencia a la pregunta anterior, por favor explique brevemente porque escogió esa escala.

   Desconozco

Escaneado con CamScanner



Encuesta

El objetivo de la presente encuesta es recolectar información acerca de las características del sistema académico Fénix que manejan los docentes del Instituto Tecnológico Superior del Azuay. Agradecemos su sinceridad y honestidad en sus respuestas, se garantiza que serán tratadas con absoluta confidencialidad, anonimato y solo se consideran para fines académicos.

Información general

Área a la que pertenece:	Tiempo de trabajo en la institución:
☐ Tecnología	☐ Menos de 1 año
☐ Administración	☐ De 1 a 2 años
☑ Docencia	☑ De 2 a 5 años
☐ Investigación	☐ Más de 5 años

1. ¿Mencione, si es de su conocimiento, qué software de desarrollo y programa gestor de base de datos se utilizaron para la construcción del sistema académico Fénix?

   Desconozco

2. En que porcentaje considera usted que el sistema académico Fénix cubre con las necesidades del instituto.

   10% 20% 30% 40% 50% 60% 70% 80% (90%) 100%

3. ¿Considera usted que el sistema académico Fénix se debería actualizar para cumplir con los nuevos parámetros que exige el Instituto Universitario?

   (Si.) No. No sabe.

4. ¿Cree usted que el sistema académico Fénix se construyó bajo alguna normativa de seguridad de la información?

   Si. No. (No sabe.)

5. Cuánto conoce usted acerca de las herramientas de ciberseguridad o seguridad de la información.

   En una escala donde 1 especifica que conoce muy poco o nada y 5 indica que es un experto.

   (1) 2 3 4 5

6. ¿Qué herramientas o características recomendaría implementar en el sistema académico Fénix? y por qué?

   No se que decir o responder.

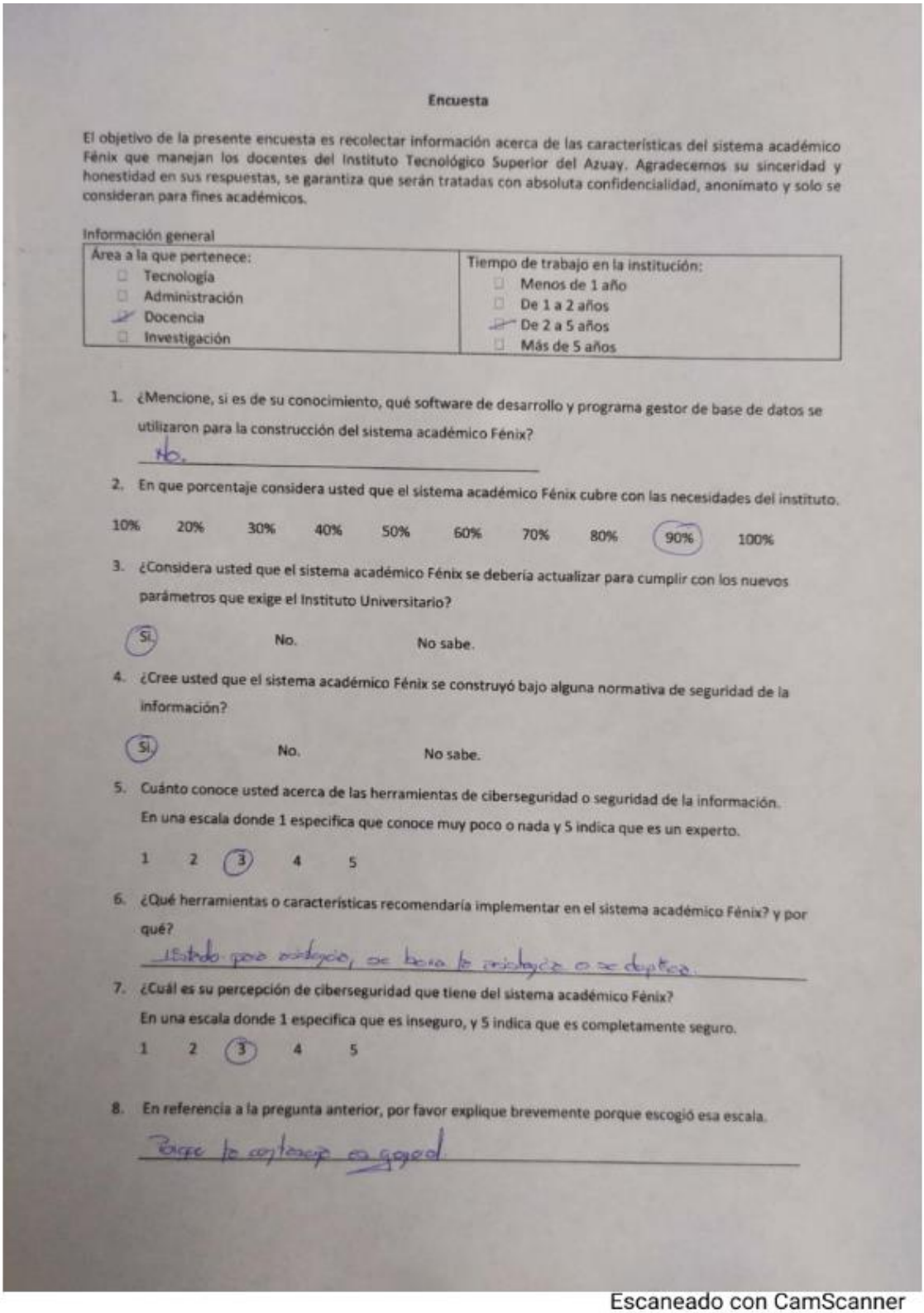
7. ¿Cuál es su percepción de ciberseguridad que tiene del sistema académico Fénix?

   En una escala donde 1 especifica que es inseguro, y 5 indica que es completamente seguro.

   (1) 2 3 4 5

8. En referencia a la pregunta anterior, por favor explique brevemente porque escogió esa escala.

   Porque desconozco del tema.



Encuesta

El objetivo de la presente encuesta es recolectar información acerca de las características del sistema académico Fénix que manejan los docentes del Instituto Tecnológico Superior del Azuay. Agradecemos su sinceridad y honestidad en sus respuestas, se garantiza que serán tratadas con absoluta confidencialidad, anonimato y solo se consideran para fines académicos.

Información general

Área a la que pertenece:	Tiempo de trabajo en la institución:
☐ Tecnología	☐ Menos de 1 año
☐ Administración	☐ De 1 a 2 años
☑ Docencia	☑ De 2 a 5 años
☐ Investigación	☐ Más de 5 años

1. ¿Mencione, si es de su conocimiento, qué software de desarrollo y programa gestor de base de datos se utilizaron para la construcción del sistema académico Fénix?

   No.

2. En que porcentaje considera usted que el sistema académico Fénix cubre con las necesidades del instituto.

   10% 20% 30% 40% 50% 60% 70% 80% (90%) 100%

3. ¿Considera usted que el sistema académico Fénix se debería actualizar para cumplir con los nuevos parámetros que exige el Instituto Universitario?

   (Si) No. No sabe.

4. ¿Cree usted que el sistema académico Fénix se construyó bajo alguna normativa de seguridad de la información?

   (Si) No. No sabe.

5. Cuánto conoce usted acerca de las herramientas de ciberseguridad o seguridad de la información.
   En una escala donde 1 especifica que conoce muy poco o nada y 5 indica que es un experto.

   1 2 (3) 4 5

6. ¿Qué herramientas o características recomendaría implementar en el sistema académico Fénix? y por qué?

   Estado para edición, se borra la misma o se duplica.

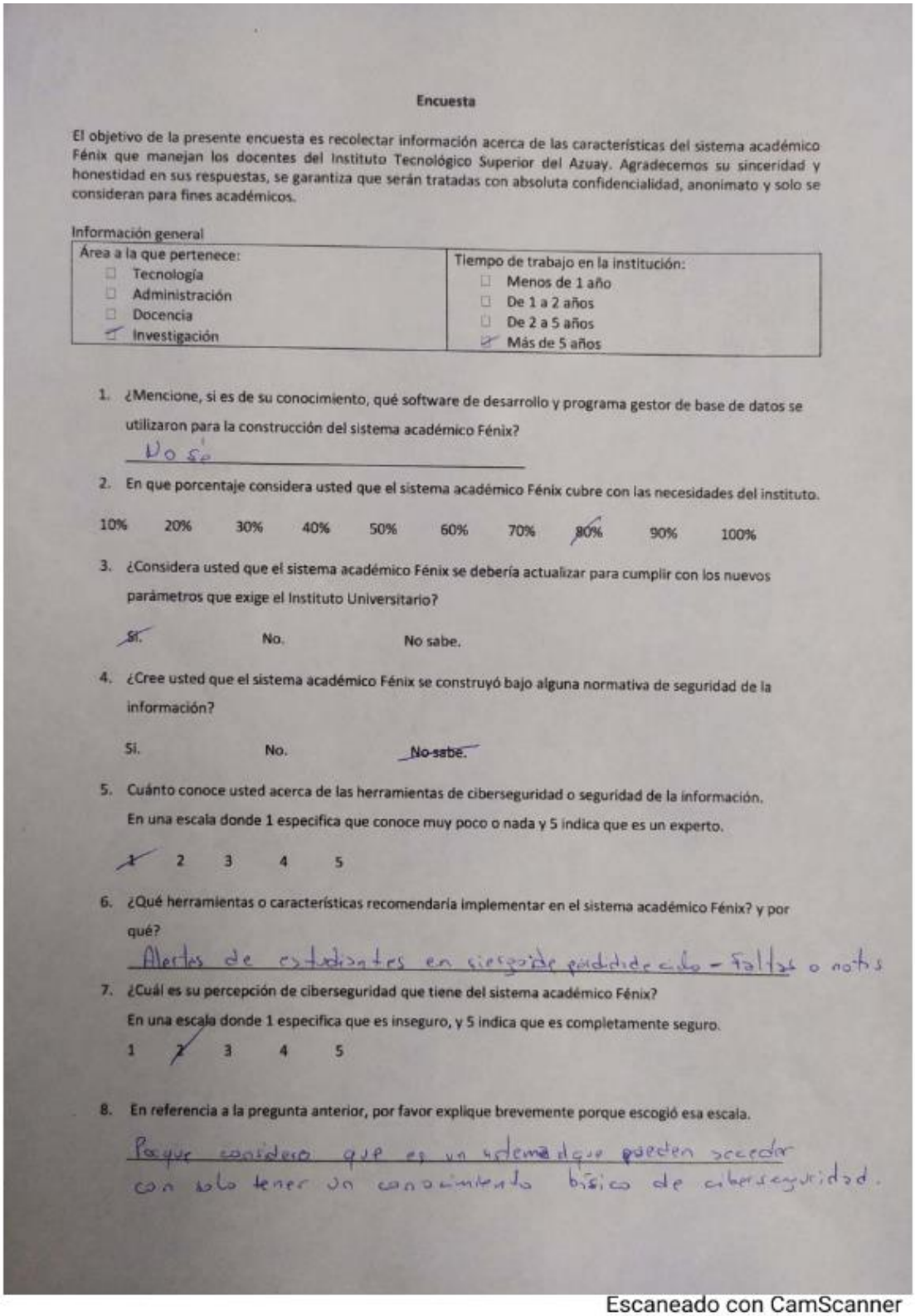
7. ¿Cuál es su percepción de ciberseguridad que tiene del sistema académico Fénix?
   En una escala donde 1 especifica que es inseguro, y 5 indica que es completamente seguro.

   1 2 (3) 4 5

8. En referencia a la pregunta anterior, por favor explique brevemente porque escogió esa escala.

   Porque lo contesce es good.

Escaneado con CamScanner



Encuesta

El objetivo de la presente encuesta es recolectar información acerca de las características del sistema académico Fénix que manejan los docentes del Instituto Tecnológico Superior del Azuay. Agradecemos su sinceridad y honestidad en sus respuestas, se garantiza que serán tratadas con absoluta confidencialidad, anonimato y solo se consideran para fines académicos.

Información general

Área a la que pertenece:	Tiempo de trabajo en la institución:
☐ Tecnología	☐ Menos de 1 año
☐ Administración	☐ De 1 a 2 años
☐ Docencia	☐ De 2 a 5 años
☑ Investigación	☑ Más de 5 años

1. ¿Mencione, si es de su conocimiento, qué software de desarrollo y programa gestor de base de datos se utilizaron para la construcción del sistema académico Fénix?

   No se

2. En que porcentaje considera usted que el sistema académico Fénix cubre con las necesidades del instituto.

   10% 20% 30% 40% 50% 60% 70% 80% 90% 100%

3. ¿Considera usted que el sistema académico Fénix se debería actualizar para cumplir con los nuevos parámetros que exige el Instituto Universitario?

   Si. No. No sabe.

4. ¿Cree usted que el sistema académico Fénix se construyó bajo alguna normativa de seguridad de la información?

   Si. No. No sabe.

5. Cuánto conoce usted acerca de las herramientas de ciberseguridad o seguridad de la información.
   En una escala donde 1 especifica que conoce muy poco o nada y 5 indica que es un experto.

   1 2 3 4 5

6. ¿Qué herramientas o características recomendaría implementar en el sistema académico Fénix? y por qué?

   Alertas de estudiantes en riesgo de perdida de ciclo - Faltas o notas

7. ¿Cuál es su percepción de ciberseguridad que tiene del sistema académico Fénix?
   En una escala donde 1 especifica que es inseguro, y 5 indica que es completamente seguro.

   1 2 3 4 5

8. En referencia a la pregunta anterior, por favor explique brevemente porque escogió esa escala.

   Porque considero que es un sistema que pueden acceder con solo tener un conocimiento básico de ciberseguridad.

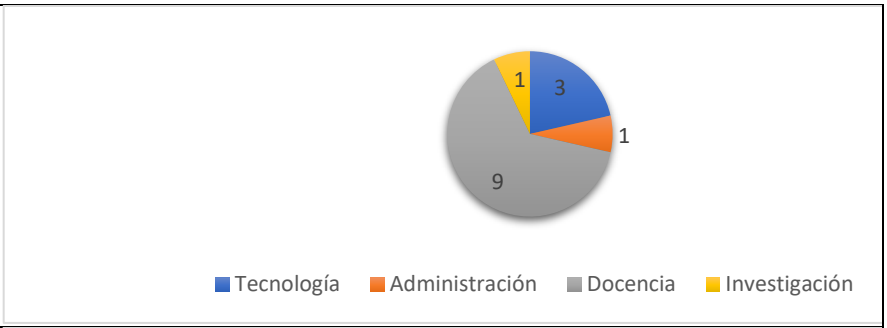
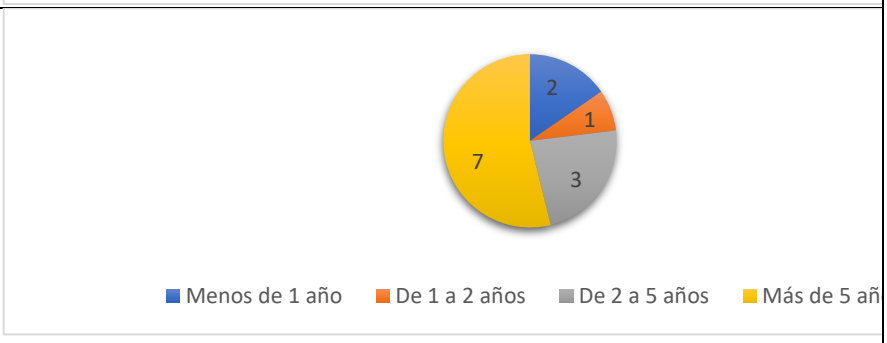
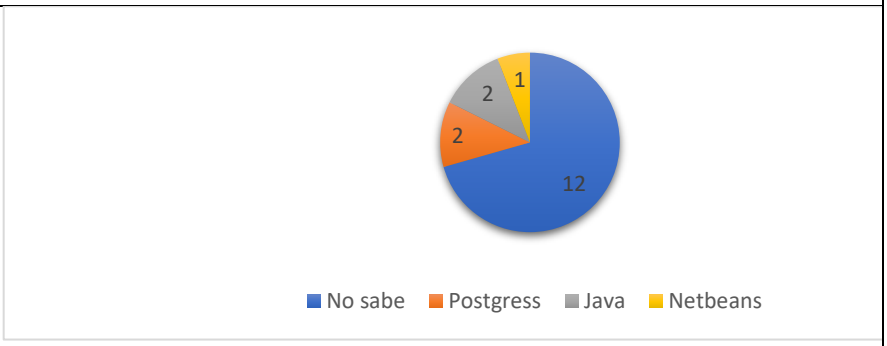
Escaneado con CamScanner

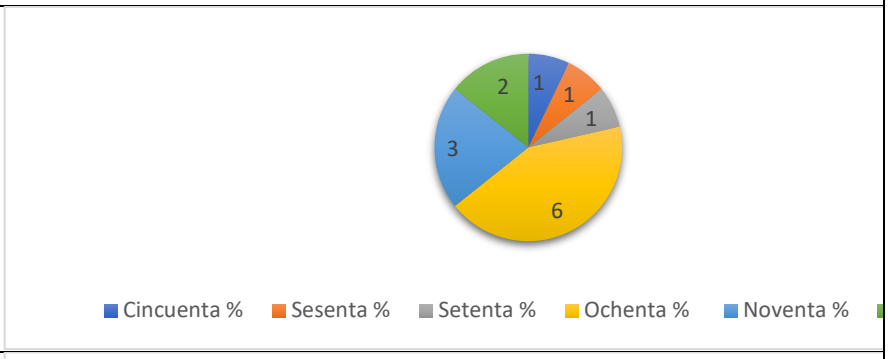
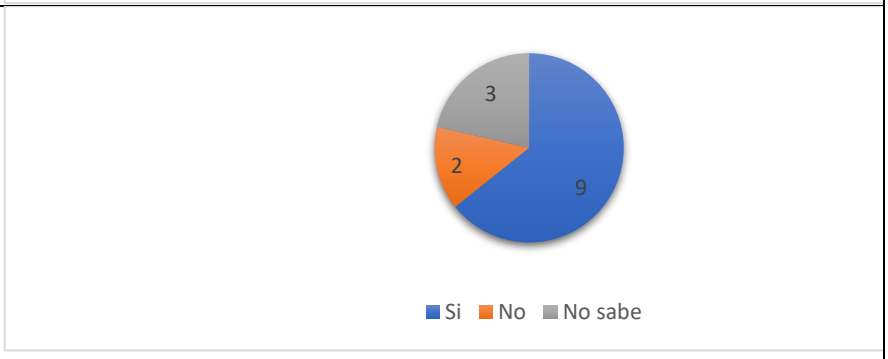
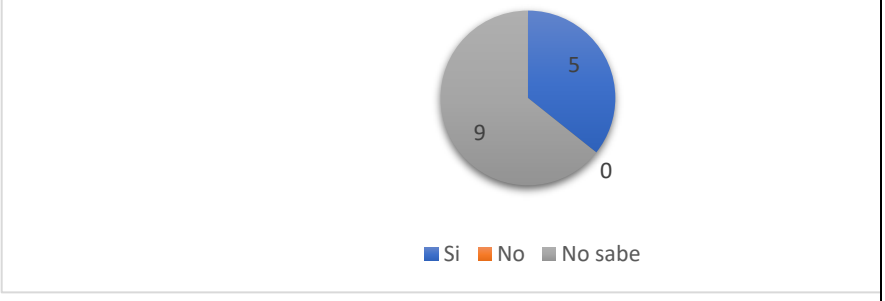
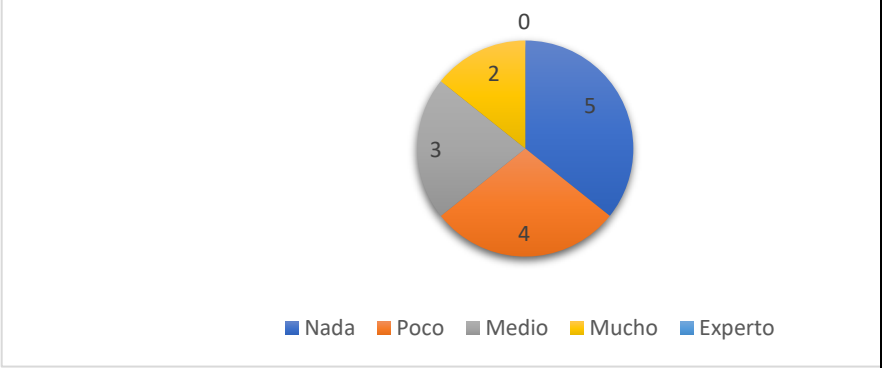
ANEXO L

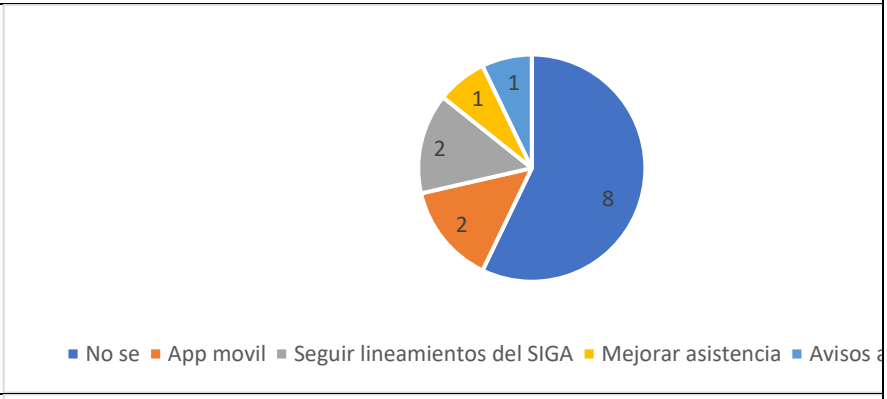
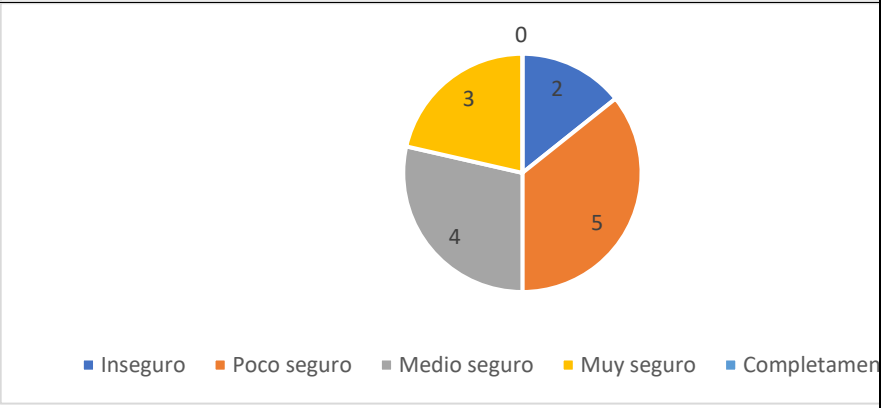
Encuesta

El objetivo de la presente encuesta es recolectar información acerca de las características del sistema académico Fénix que manejan los docentes del Instituto Tecnológico Superior del Azuay. Agradecemos su sinceridad y honestidad en sus respuestas, se garantiza que serán tratadas con absoluta confidencialidad, anonimato y solo se consideran para fines académicos.

Resultados de las encuestas

Área a la que pertenece: ☐ Tecnología ☐ Administración ☐ Docencia ☐ Investigación	
Tiempo de trabajo en la institución: ☐ Menos de 1 año ☐ De 1 a 2 años ☐ De 2 a 5 años ☐ Más de 5 años	
¿Mencione, si es de su conocimiento, qué software de desarrollo y programa gestor de base de datos se utilizaron para la construcción del sistema	

académico Fénix?	
En qué porcentaje considera usted que el sistema académico Fénix cubre con las necesidades del instituto.	
¿Considera usted que el sistema académico Fénix se debería actualizar para cumplir con los nuevos parámetros que exige el Instituto Universitario?	
¿Cree usted que el sistema académico Fénix se construyó bajo alguna normativa de seguridad de la información?	
Cuánto conoce usted acerca de las herramientas de ciberseguridad o seguridad de la información. En una escala donde 1 especifica que conoce muy poco o nada y 5	

indica que es un experto	
¿Qué herramientas o características recomendaría implementar en el sistema académico Fénix? y por qué?	
¿Cuál es su percepción de ciberseguridad que tiene del sistema académico Fénix? En una escala donde 1 especifica que es inseguro, y 5 indica que es completamente seguro.	
En referencia a la pregunta anterior, por favor explique brevemente porque escogió esa escala.	• Desconocimiento en temas de seguridad de la información. • No exige parámetros de seguridad informática. • Si se han realizado pruebas de pentesting, validación, encriptación de base de datos. • Si se ha realizado pruebas de uso, testing de usuario, validaciones en pruebas y producción. • Se dispone de actualizaciones regulares. • Acceso de manera facil. • Falta de recursos economicos para proveer seguridad. • Manejo de usuario y contraseñas debil. • Se puede acceder al sistema facilmente.