

UNIVERSIDAD TÉCNICA DE AMBATO



CENTRO DE POSGRADOS

PROGRAMA DE MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN COHORTE 2022

Tema: MODELO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA
INFORMACIÓN EN LA RED INFORMÁTICA, BASADO EN LA ISO/IEC
27002.

Trabajo de Titulación, previo a la obtención del Título de Cuarto Nivel de Magister
en Tecnologías de la Información Mención Seguridad de Redes y Comunicaciones.

Modalidad del Trabajo de Titulación: Proyecto de Titulación con Componente de
Investigación Aplicada.

Autor: Ingeniero Cristian Javier Saltos Ponce.

Director: Ingeniero David Omar Guevara Aulestia Magister

Ambato – Ecuador

2023

A la Unidad Académica de Titulación del Centro de Posgrados

El Tribunal receptor del Trabajo de Titulación, presidido por el Ingeniero Oscar Fernando Ibarra Torres Magister, Delegado por el Ingeniero Héctor Fernando Gómez Alvarado PhD, Director del Centro de Posgrados e integrado por los señores: *Ingeniero José Miguel Ocaña Chiluisa PhD e Ingeniera Lorena Isabel Barona López PhD*, designados por la Unidad Académica de Titulación del Centro de Posgrados de la Universidad Técnica de Ambato, para receptor el Trabajo de Titulación con el tema: “*Modelo de gestión de incidentes de seguridad de la información en la red informática, basado en la ISO/IEC 27002*”, elaborado y presentado por el señor Ingeniero Cristian Javier Saltos Ponce, para optar por el Título de cuarto nivel de Magíster en Tecnologías de la Información mención Seguridad de Redes y Comunicaciones; una vez escuchada la defensa oral del Trabajo de Titulación, el Tribunal aprueba y remite el trabajo para uso y custodia en las bibliotecas de la UTA.

Ing. Oscar Fernando Ibarra Torres Mgtr.
Presidente y Miembro del Tribunal

Ing. José Miguel Ocaña Chiluisa PhD.
Miembro del Tribunal

Ing. Lorena Isabel Barona López PhD.
Miembro del Tribunal

AUTORÍA DEL TRABAJO DE TITULACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Titulación presentado con el tema: Modelo de gestión de incidentes de seguridad de la información en la red informática, basado en la ISO/IEC 27002, le corresponde exclusivamente al: Ing. Cristian Javier Saltos Ponce, Autor bajo la Dirección del Ing. David Omar Guevara Aulestia, Mg., Director del Trabajo de Titulación, y el patrimonio intelectual a la Universidad Técnica de Ambato.

Ingeniero Cristian Javier Saltos Ponce

c.c.: 0504232240

AUTOR

Ingeniero David Omar Guevara Aulestia Magister

c.c.: 1802605749

DIRECTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que el Trabajo de Titulación, sirva como un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los Derechos de mi trabajo, con fines de difusión pública, además apruebo la reproducción de este, dentro de las regulaciones de la Universidad.

Ingeniero Cristian Javier Saltos Ponce
c.c.: 0504232240

INDICE GENERAL DE CONTENIDOS

PORTADA.....	i
A la Unidad Académica de Titulación del Centro de Posgrados.....	ii
AUTORÍA DEL TRABAJO DE TITULACIÓN	iii
DERECHOS DE AUTOR	iv
INDICE GENERAL DE CONTENIDOS.....	v
ÍNDICE DE TABLAS	vii
ÍNDICE DE FIGURAS.....	x
AGRADECIMIENTO	xii
DEDICATORIA	xiii
RESUMEN EJECUTIVO	xiv
CAPÍTULO I.....	1
EL PROBLEMA DE INVESTIGACIÓN.....	1
1.1. Introducción.....	1
1.2. Justificación	3
1.3. Objetivos.....	5
CAPITULO II	7
MARCO TEORICO.....	7
2.1 ANTECEDENTES INVESTIGATIVOS.....	7
2.2 FUNDAMENTACIÓN CIENTÍFICA	13
CAPITULO III.....	32
MARCO METODOLÓGICO	32
3.1. Tipo de investigación.....	32
3.2. Población o muestra.....	32
3.3. Recolección de información	33

3.4. Procesamiento de la información.....	34
CAPITULO IV.....	35
RESULTADOS Y DISCUSIÓN	35
4.1 Estado inicial de la institución.....	35
CAPÍTULO V.....	71
CONCLUSIONES, RECOMENDACIONES, BIBLIOGRAFÍA, ANEXOS. ..	71
5.1. Conclusiones.....	71
5.2. Recomendaciones	72
5.3. Bibliografía.....	73
5.4. Anexos	77
CAPÍTULO VI.....	84
PROPUESTA.....	84
6. DATOS INFORMATIVOS.....	84
6.1. Título.....	84
6.2. Descripción	84
6.3. Desarrollo de la propuesta	86

ÍNDICE DE TABLAS

Tabla 1.....	17
Tabla 2.....	19
Tabla 3.....	22
Tabla 4.....	26
Tabla 5.....	35
Tabla 6.....	44
Tabla 7.....	45
Tabla 8.....	46
Tabla 9.....	49
Tabla 10.....	52
Tabla 11.....	52
Tabla 12.....	55
Tabla 13.....	59
Tabla 14.....	60
Tabla 15.....	61
Tabla 16.....	61
Tabla 17.....	62
Tabla 18.....	63

Tabla 19.....	68
Tabla 20.....	87
Tabla 21.....	87
Tabla 22.....	88
Tabla 23.....	89
Tabla 24.....	90
Tabla 25.....	92
Tabla 26.....	94
Tabla 27.....	95
Tabla 28.....	97
Tabla 29.....	100
Tabla 30.....	101
Tabla 31.....	102
Tabla 32.....	104
Tabla 33.....	105
Tabla 34.....	107
Tabla 35.....	117
Tabla 36.....	131
Tabla 37.....	145
Tabla 38.....	145
Tabla 39.....	146
Tabla 40.....	147
Tabla 41.....	149
Tabla 42.....	150
Tabla 43.....	151
Tabla 44.....	152
Tabla 45.....	154
Tabla 46.....	156
Tabla 47.....	157
Tabla 48.....	158
Tabla 49.....	159

ÍNDICE DE FIGURAS

Figura 1	14
Figura 2	15
Figura 3	28
Figura 4	29
Figura 5	48
Figura 6	58
Figura 7	58
Figura 8	70
Figura 9	70
Figura 10	70
Figura 11	71
Figura 12	109
Figura 13	109
Figura 14	111
Figura 15	112
Figura 16	112
Figura 17	113
Figura 18	113
Figura 19	114
Figura 20	114
Figura 21	115
Figura 22	115
Figura 23	116
Figura 24	116
Figura 25	117
Figura 26	119
Figura 27	120
Figura 28	121
Figura 29	123
Figura 30	123
Figura 31	124

Figura 32	125
Figura 33	126
Figura 34	127
Figura 35	128
Figura 36	129

AGRADECIMIENTO

A la Universidad Técnica de Ambato por su compromiso con la excelencia académica. A los excelentes docentes por incentivar el aprendizaje en los retos planteados, su orientación y dedicación ha sido clave para mi formación.

A mi director de tesis Ing. David Omar Guevara Aulestia, Mg. por su apoyo incondicional y predisposición en momentos difíciles del desarrollo de esta investigación permitiéndome crecer personal y profesionalmente.

A la Facultad de Ingeniería en Sistemas Electrónica e Industrial de la UTA, en especial a la Ing. Pilar Urrutia, Mg. decana de la facultad, por consentir la elaboración de mi proyecto en mi querida FISEI donde me forme. De manera especial a los colaboradores del área de TIC's por su ayuda y colaboración.

Agradezco a un gran amigo, Ing. Julio Balarezo, PhD., quien sin reparo me brindó su apoyo incondicional compartiendo sus consejos y orientación, dándome fuerzas para continuar formándome personal y académicamente.

A mis compañeros de maestría quienes sin reparo me brindaron un apoyo incondicional en cada uno de los retos presentados, de manera especial a mi compañero Fernando Moya.

Cristian Javier Saltos Ponce

DEDICATORIA

Quiero dedicar el presente trabajo a Dios y a la Virgen de Baños de Agua Santa, quienes me han protegido a mí y a mi familia, por darnos salud, permitiéndome gozar del amor de mis padres, permitiéndome concluir una meta más en mi vida personal y profesional.

Con profundo amor y cariño, a mis dos pilares fundamentales en mi vida mis padres, Luis Saltos y Emperatriz Ponce. Su ejemplo de trabajo arduo y dedicación en momentos difíciles ha sido mi principal inspiración por progresar personal y profesionalmente, gracias por los valores y principios que forjan el día a día de mi vida.

A la Facultad de Ingeniería en Sistemas Electrónica e Industrial de la UTA quien me abrió las puertas con mis estudios, lugar que llevo en mi corazón donde llevo a ser mi segundo hogar el cual tengo mucho cariño y respeto, en el cual encontré personas que estuvieron presentes en mi proceso continuo de aprendizaje y formación, quienes se convirtieron en mi segunda familia.

Cristian Javier Saltos Ponce

UNIVERSIDAD TÉCNICA DE AMBATO
CENTRO DE POSGRADOS
MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN
COHORTE 2022

TEMA:

MODELO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN EN LA RED INFORMÁTICA, BASADO EN LA ISO/IEC 27002.

MODALIDAD DE TITULACIÓN: *Proyecto de Titulación con Componente De Investigación Aplicada y de Desarrollo.*

AUTOR: *Ingeniero Cristian Javier Saltos Ponce.*

DIRECTOR: *Ingeniero David Omar Guevara Aulestia Magister*

FECHA: *de dos mil veinte y tres*

RESUMEN EJECUTIVO

Actualmente las instituciones de educación superior han potenciado sus estructuras académicas y administrativas dando cabida a la demanda por parte de la comunidad universitaria que se va sumando a la educación superior. En este sentido el presente proyecto de titulación expone el desarrollo de un modelo de gestión de incidentes de seguridad de la información en la red informática, basado en la ISO/IEC 27002, con la finalidad de asegurar la seguridad su información, dentro de la Facultad de Ingeniería en Sistemas Electrónica e Industrial (FISEI) de la UTA.

La importancia de esta investigación es dar cumplimiento a los siguientes objetivos, primero analizar los riesgos de vulnerabilidad de la información del departamento de administración de redes, luego identificar los aspectos a tener en cuenta en la definición de un modelo de gestión de incidentes de seguridad de la información, una vez identificado los posibles riesgos se procede a diseñar el modelo del sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27002.

Para desarrollar el presente trabajo de investigación se utilizó la metodología de investigación cualitativa con un enfoque exploratorio, empleando además una investigación de campo mediante la realización de entrevistas, la observación, y la

ejecución de pruebas de penetración externas sobre la red y servicios de la FISEI de la UTA.

Con la ejecución adecuada de las pruebas de escaneo de puertos se logró detectar de forma eficiente las vulnerabilidades que afectan a la red y servicios de la FISEI de la UTA, lo cual permitió desarrollar un modelo de gestión de incidentes de seguridad de la información en la red informática.

Para mitigar las vulnerabilidades que afectan a la red de la FISEI así como minimizar los riesgos a los que su infraestructura se encuentra expuesta, es importante que la institución se acoja a lo dispuesto en la Norma ISO/IEC 27002 con el objetivo de asegurar en todo momento la integridad, disponibilidad y confidencialidad de la información.

DESCRIPTORES: *RIESGOS, AMENAZAS, NORMAS, ESTÁNDARES, ISO/IEC 27002, INTRUSOS, ESCANEAO, PUERTOS, MODELO, GESTIÓN, SEGURIDAD INFORMÁTICA, VULNERABILIDADES.*

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1. Introducción

En la actualidad uno de los temas de interés en cualquier institución pública o privada es poder mejorar la seguridad de su información. Sin embargo, muchas veces no le dan la importancia que realmente merece y en un momento determinado sucede un incidente en el que la información se encuentra en peligro y es ahí cuando deciden tomar acciones para que no vuelva a ocurrir (Briceño, 2021). La importancia de los equipos informáticos y la información generada por cualquier institución en general representa la continuidad de las funciones, por lo tanto, se debe proteger contra cualquier tipo de ataque informático que quiera infringir la seguridad y causar daños a la misma.

Para la presente investigación se hace referencia al caso de estudio de una Universidad Pública del Ecuador, mismo que será desarrollado en la Universidad Técnica de Ambato (UTA) para la Facultad de Ingeniería en Sistemas Electrónica e Industrial (FISEI), que puede ser tomado como referencia y punto de partida para otras investigaciones y universidades. La institución cuenta con varios usuarios entre estudiantes, docentes y personal administrativo que genera información valiosa, misma que hace uso de los equipos informáticos conectados a la red informática de la Facultad, razón por la cual se ha presentado la motivación de la mejora de procesos y gestión de la seguridad de la información.

Actualmente la era digital y la tecnología atraviesan por cambios constantes y es importante conocer los riesgos existentes a los cuales puede ser víctima una organización, así como las herramientas necesarias para contrarrestar y prevenir este tipo de ataques. En el presente trabajo se presente un Sistema de Gestión de Seguridad de la Información (SGSI), aplicando los controles propuestos por la ISO/IEC 27002, para reducir las brechas existentes en los temas de seguridad de la información (ISO/IEC 27002, 2020).

Un análisis adecuado de vulnerabilidades permite a cualquier institución determinar las acciones que debe ejecutar para mitigar las mismas y así evitar ser víctima de un ataque informático, en la actualidad se ha vuelto bastante popular y rentable para los delincuentes este tipo de robos informáticos.

Por lo antes mencionado, surge la necesidad de desarrollar el presente trabajo de investigación, mediante el cual se propone un modelo de gestión de incidentes de seguridad de la información, que permita mitigar riesgos y fortalecer la información sensible de la institución antes mencionada a fin de mejorar los niveles de seguridad.

El presente trabajo de investigación tiene una estrategia cualitativa, dado a que emite juicios de valor correspondiente al riesgo y seguridad de la información en relación a mejorar la gestión del departamento de Administración de Redes de la FISEI de la UTA.

Como colaboradores para el presente proyecto de investigación se considera a la Dirección de Tecnología de Información y Comunicación (DITIC), ya que es un departamento de la UTA que apoya el desarrollo del presente modelo de gestión, que se adapte a las políticas y normativas de seguridad de la información establecidas por dicho departamento y a la medida de las necesidades de la FISEI.

El Capítulo I contiene la introducción y justificación del tema de investigación. Además, se detalla los objetivos planteados como es el general y los específicos a desarrollarse.

El Capítulo II contiene los antecedentes investigativos junto a una detenida revisión literaria, fundamentación científica mismo que cuenta con información importante relacionado al tema del proyecto de investigación.

El Capítulo III describe el contenido a detalle del marco metodológico, tipo de investigación, población o muestra, recolección de información, procesamiento de la información.

El Capítulo IV contiene los resultados y discusión, estado inicial de la institución, evaluación de riesgos.

El Capítulo V contiene las conclusiones, recomendaciones, bibliografía y los respectivos anexos que dan sustento a la investigación.

El Capítulo VI contiene la propuesta planteada, la modalidad de titulación, proyecto de titulación, con componente de investigación aplicada y desarrollo.

1.2. Justificación

Debido a la situación de emergencia sanitaria por el COVID 19 que atravesó el país, muchas instituciones migraron la manera de conectarse a su trabajo, negocio, o educación a forma virtual con la finalidad de mantener la continuidad de sus labores, lo cual ha llevado a que se ponga más interés en reforzar la seguridad de la red (Gracia, 2021).

América Latina está posicionada en un nivel de desarrollo intermedio respecto a otras regiones del mundo con un índice de 49.92% estos datos muestra un rezago respecto a Europa Occidental (con un índice de 71.06) y América del Norte (80.85) en términos de desarrollo de migración a un ecosistema digital, lo cual indica que incluido Ecuador no se encuentra preparado ante una eventual emergencia para la continuidad laboral y educativo (Chomali, 2020).

Actualmente la FISEI no cuenta con una metodología ágil que permita regular el control de riesgos que se puedan materializar en los activos informáticos, la falta de procedimientos que garanticen el buen funcionamiento de los equipos informáticos. La infraestructura de red son factores que con el pasar de los años empiezan a presentar fallos físicos y lógicos dando lugar a la presencia de

vulnerabilidades y amenazas los cuales deben ser solucionados con la brevedad que esta amerita. En otros casos controlar que su impacto sea leve, para que la institución no detenga sus actividades tanto académicas como administrativas perjudicando la imagen de la institución.

Por estos motivos, es de gran importancia desarrollar esta investigación, al crear un marco estratégico para reforzar la seguridad en cuanto al acceso a la información conectada a una red con salida a internet e identificar los posibles impactos potenciales que amenazan a la institución construyendo la capacidad de dar una respuesta clara que salvaguarde los intereses y la imagen de la FISEI.

El trabajo de investigación es factible en el departamento de Administración de redes de la FISEI ya que se cuenta con el consentimiento y aprobación del Decanato y la Dirección de Tecnología de Información y Comunicación DITIC de la UTA, lo cual permite tener la apertura necesaria con el personal encargado de la Administración de Redes para conseguir información y garantizar que los resultados serán reales y de utilidad para la toma de decisiones en dicha entidad.

El impacto que la investigación tiene por resultado fortalecer las defensas contra amenazas cibernéticas y vulnerabilidades potenciales, garantizando la confidencialidad, integridad y disponibilidad de la información crítica de la organización.

La originalidad de esta investigación reside en la aplicación de la normativa ISO/IEC 27002 para la gestión de seguridad de la información. Lo distintivo del presente modelo de gestión radica en la adaptación precisa de los controles y buenas prácticas recomendadas por la normativa.

Como beneficiario del presente proyecto de investigación se encuentra la FISEI de la UTA, en el cual se propone la implementación de mejores prácticas destinadas a la gestión de la información, ante posibles incidentes de seguridad informática que puedan materializarse donde reducir tiempos de respuesta y

tener una guía para evitar que las actividades de la institución se paralicen es lo principal.

Se puede mencionar que desde el punto de vista económico el proyecto es viable ya que no genera, algún tipo de inversión o uso de recursos extras de la institución únicamente consta de trabajo del investigador y la colaboración del personal encargado del departamento de redes, por lo mismo es de gran ayuda para solventar problemas reales en el ámbito social garantizando la concientización de la importancia de estos temas en la actualidad.

Los resultados de la investigación estarán estrictamente protegidos por lo que se difundirá lo necesario para entender como fue aplicada la técnica de gestión de seguridad de la información.

1.3. Objetivos

1.3.1. General

Establecer un modelo de Gestión de incidentes de seguridad de la información basado en la norma ISO/IEC 27002 para la Facultad de ingeniería en Sistemas Electrónica e Industrial de la UTA.

1.3.2. Específicos

- Analizar los riesgos de vulnerabilidad de la información del departamento de administración de redes.

- Identificar los aspectos a tener en cuenta en la definición de un modelo de gestión de incidentes de seguridad de la información.
- Modelar el sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27002.
- Desarrollar la propuesta de solución en el ámbito de un caso de estudio en la FISEI de la UTA.

CAPITULO II

MARCO TEORICO

2.1 ANTECEDENTES INVESTIGATIVOS

Con el pasar del tiempo los ataques informáticos han venido desarrollando nuevas estrategias que se han convertido en formas de ataque a las instituciones tanto públicas como privadas estas pueden ser amenazas externas o internas, por lo que ha llevado a las distintas entidades a preocuparse por temas de seguridad de la información, así como su adecuada gestión para de esta manera garantizar la continuidad de sus operaciones en caso de que ocurra algún tipo de ataque.

Durante la pandemia de COVID-19 se ha incrementado la tasa de ataques con impactos potenciales a organizaciones y personas lo que se convirtió en una fuente de preocupación. La tendencia de ataques cibernéticos genera un aumento de vulnerabilidad donde surgieron diversos grados de impacto lo que obligo a incluir la adopción de medidas de seguridad de la información. Contratar servicios en línea a medida que la pandemia transcurría fue una alternativa muy aceptada para diferentes actividades tanto de trabajo, estudio, ocio y negocios dando lugar a la exposición y robo de datos confidenciales que no se encontraban protegidos correctamente donde los delitos cibernéticos tenían la ventaja (Suastegui Jaramillo, 2022).

En el paralelismo internacional se han efectuado trabajos de investigación con propósitos afines al que se pretende investigar, el cual se detalla a continuación:

En el año 2022, se elaboró el trabajo de investigación “Diseño de Evaluación de Madurez de Ciberseguridad usando NISTCSF, CIS CONTROLS v8 e ISO/IEC 27002”, desarrollado por I. Bashofi y M. Salman. Caso de estudio: La Organización XYZ es una de las instancias gubernamentales que gestionan las infraestructuras críticas de INDONESIA, permitió un marco de madurez donde se evidencia el desempeño de las TIC en la organización. En este trabajo concluye que la investigación con relación a la norma ISO/IEC 27002 se ajusta a las necesidades de la organización dando alertas de seguridad mismas que son contrarrestadas por los controles de la norma (Salman, 2022).

En el año 2022, se elaboró el trabajo de investigación “Análisis de gestión de riesgos de seguridad utilizando el método de análisis de efectos y modos de falla (FMEA) y mitigación utilizando ISO/IEC 27002: 2013 para la agencia en el gobierno del distrito” desarrollado por G. Muhamad Nur, R. Lusi y F. Fitroh. Esta investigación le permitió identificar riesgos, realizar una evaluación y proporcionar recomendaciones de mitigación de riesgos basadas en el estándar ISO/IEC 27002. El autor concluye que los resultados del estudio ofrecerán material para analizar y realizar mejoras y controles de seguridad para evitar amenazas a los activos informáticos para posteriormente brindar recomendaciones para mitigar los riesgos basados en la norma adaptada a la organización (G. Muhamad Nur, 2022).

En el año 2022, se elaboró el trabajo de investigación “Mejor comunicación de evaluación de seguridad: combinación de controles ISO/IEC 27002 con diagramas de secuencia UML” desarrollado por Sechi, Fabien, Bjorn, Per-Arne, Kilyukh. Caso de estudio: Central nuclear de Ucrania, permitió ejecutar pruebas y evaluación de seguridad ISO/IEC 27002 asignando los respectivos controles de seguridad a los escenarios de la red empresarial. Este trabajo concluye que dependiendo de la planta y magnitud empresarial la visualización de diagramas de secuencia y controles de seguridad mejora la evaluación de seguridad (F. Sechi, 2022).

Existe un índice de ataques a la seguridad de la información a nivel global a continuación se presenta que puesto ocupa Ecuador con referencia su seguridad informática en los últimos años:

Según el Índice Mundial de Ciberseguridad 2020, Ecuador se encuentra en el puesto 19 con una puntuación global a nivel de la Región de las Américas en los países con más índices de ataques cibernéticos. Estos países van mejorando sus estrategias de seguridad en el que se pueden abordar para fortalecer el ecosistema digital. El Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) apoya a la seguridad de las redes de telecomunicaciones, a través de la coordinación nacional e internacional a lograr usos más seguros de estas redes, de ahí la importancia que toda organización tanto pública como privada debe considerar el correcto funcionamiento de sus actividades (ITU, 2020).

En los últimos años ECUADOR ha hecho algunos esfuerzos por mejorar la conectividad a internet de la población con el objetivo de acelerar el desarrollo

económico y social, la estrategia fue liderada por el MINTEL en conjunto con el Comité Nacional de Ciberseguridad donde consta de pilares fundamentales que son la Gobernanza y coordinación nacional, prevención y lucha contra la cibercriminalidad. Todo estos pilares se desarrollan con el objetivo de fomentar la continuidad de la organización ya que se menciona que es un tema de vital importancia y el Gobierno de turno apoya la construcción de las estrategias antes mencionadas (Mintel, 2022).

En los últimos años se han adoptado los usos de buenas prácticas de seguridad las que han permitido a las organizaciones consolidar una correcta defensa sólida que combata contra ataques y vulneraciones informáticas. En Ecuador esto ocurre independientemente del tamaño de la organización a continuación se presenta varias investigaciones que se relacionan al tema de la presente investigación a través de los años:

La necesidad de proteger la información surge dado al alto crecimiento de ataques informáticos y más aún cuando se maneja información delicada como es el caso de la “Empresa Municipal de Agua Potable y Alcantarillado de Ambato”, dicho proyecto se basó en la norma internacional “ISO/IEC 27001:2013” de la misma manera hace uso de la metodología de análisis y gestión de riesgos de información “MAGERIT” utilizando métodos estadísticos se comprueba el nivel de impacto del proyecto y tomar las medidas de seguridad pertinentes (Moya, 2023).

En el proyecto de investigación de Aranda Juan, “EVALUACIÓN DE RIESGOS INFORMÁTICOS Y DISEÑO DE UN PLAN DE CONTINGENCIA PARA EL ÁREA DE TECNOLOGÍA DE LA EMPRESA IMPORTADORA ALVARADO VÁSCONEZ CIA. LTDA., UBICADA EN LA CIUDAD DE AMBATO.” realiza una evaluación de riesgos informáticos en el que hace uso de la metodología MAGERIT misma que le permitió realizar una gestión de riesgos haciendo uso de la norma ISO/IEC 27001, donde realiza un análisis cualitativo y cuantitativo que le permite tener un panorama claro de lo que se necesita hacer para una buena toma de decisiones y brindar la continuidad del negocio que toda organización requiere (Aranda, 2022).

Para la obtención del título de cuarto nivel Cedeño María hace un proyecto sobre “DETECCIÓN DE VULNERABILIDADES MEDIANTE PRUEBAS DE

PENETRACIÓN A LA RED DE SERVIDORES Y SERVICIOS DEL INSTITUTO SUPERIOR TECNOLÓGICO SUCRE”. En este proyecto se realiza la detección de vulnerabilidades a través de pruebas de penetración en la red de la institución lo cual demuestra un plan de mejora que le permitió mitigar las vulnerabilidades identificadas mediante pruebas de penetración en la red, también se puede apreciar que utiliza una investigación cualitativa demostrando una exploración de campo a través de entrevistas para mayor enfoque exploratorio (Cedeño, 2022).

Guacanes Marco, en el año 2022, en su proyecto de investigación, “PROPUESTA DE DISEÑO DE UN SGSI BASADO EN LA NORMA ISO/IEC 27001 CASO DE ESTUDIO LA EMPRESA ULTRALINK”, en la ciudad de Quito donde utilizó un modelo de buenas prácticas de seguridad las cuales darán a la empresa las garantías necesarias para que la seguridad de la información posea las herramientas necesarias que genere confianza en los interesados. El autor hace un estudio del estado de la empresa donde detecta las brechas de seguridad para atacar las vulnerabilidades y disminuir el riesgo de que se materialicen, esto ayuda a generar conocimiento y reaccionar con agilidad disminuyendo el tiempo de actuar ante una amenaza (Marco, 2022).

Grande Christian, en el año 2021, en su proyecto de investigación, propone un “DESARROLLO DE PROCESOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y BUENAS PRÁCTICAS PARA LA GESTIÓN ACADÉMICOADMINISTRATIVA EN EL INSTITUTO SUPERIOR TECNOLÓGICO SUCRE DE LA ZONAL 9 DEL DISTRITO METROPOLITANO DE QUITO”, en el cual hace un análisis sobre los procesos del área de TI de la institución a través de la metodología COBIT 2019 enfocándose en encontrar puntos críticos que se puedan corregir. Concluye un manual que resalta los resultados del análisis y sus propuestas de mejora que buscan monitorear la calidad aplicadas a cada proceso (Christian, 2021).

Camacho Victoria, en el año 2021, en su proyecto de investigación, “DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, BASADO EN LA NORMA ISO/IEC 27001:2013, PARA UNA FÁBRICA DE CUERO Y CALZADO”, en este proyecto desarrollado en la ciudad de Quito el autor diseña un SGSI ajustados a las necesidades de la empresa en base a la metodología

MAGERIT, misma recomienda realizar la valoración de activos recolectando toda la información necesaria con la finalidad de encontrar los riesgos que no han sido tratados en la investigación. El autor concluye que llevó a cabo el análisis de riesgos presentando un documento que detalla un conjunto de políticas en base al Anexo A de la norma ISO/IEC 27001:2013 (Camacho, 2021).

Alfonso Portilla, en el año 2020, en su proyecto de investigación, “DISEÑO DE UNA POLÍTICA DE SEGURIDAD PARA LA INFRAESTRUCTURA DE RED DE LA UNIVERSIDAD CENTRAL DEL ECUADOR BASADA EN LA ISO/IEC 27002:2013”, en la ciudad de Quito. El autor realizó un análisis de la política de seguridad existente en la institución para en base a esta actualizarla misma que le permitió establecer los controles necesarios para aplicar buenas prácticas con el objetivo de tratar los incidentes de seguridad. El autor concluye que seleccionó controles específicos de la Norma ISO IEC 27002:2013 además de buenas prácticas para la gestión de riesgos mismos que le sirvió para mitigar estas amenazas en la institución (Hernández, 2020).

Patricio Mendoza, en el año 2020, en su proyecto de investigación, “PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA ALPHA TECHNOLOGIES CIA. LTDA CON LA NORMA ISO/IEC 27001:2011”, en la ciudad de Quito. El autor propone conocer las deficiencias que presenta la empresa hace un análisis de la situación actual para categorizar el problema estableciendo métricas de análisis basado en metodologías ágiles. Con ayuda de entrevistas al personal encargado del área de TICS, hace una revisión de documentos relacionados a la seguridad de la información proporcionados por dicha empresa. El autor concluye en diseñar un plan de seguridad informático que le permitió brindar apoyo a los clientes brindando soluciones inmediatas (Mendoza, 2020).

Wilson Cuenca en el año 2019, en su proyecto de investigación, “GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001 Y SU INCIDENCIA EN LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR DE LA CIUDAD DE MACHALA”, en el que utilizó la norma de seguridad para analizar las políticas y la seguridad de la información mismo que tiene por objetivo disminuir pérdidas de información basados en las necesidades del departamento de TICS. El autor concluye que la norma le permitió identificar

brechas de seguridad en algunos activos por ende definió controles y políticas de seguridad de la norma para la protección de la información de la Universidad de Machala (Wilson, 2019).

Pilla Julio, en el año 2019, en su proyecto de investigación, “DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN DE LA COOPERATIVA DE AHORRO Y CRÉDITO CHIBULEO LTDA., BASADO EN LA NORMA ISO/IEC 27002:2013”. El autor propone el desarrollo de un análisis de la normativa internacional, para el diseño de una política de seguridad de la información y proteger los activos críticos de la institución. El autor concluye en el desarrollo de una matriz de riesgo de seguridad en la que identificó las vulnerabilidades y amenazas de los activos informáticos previamente valorados con las autoridades de la institución, donde para mitigar los eventos críticos identifico los controles adecuados acorde a las incidencias de seguridad (Julio, 2019).

Aza Anderson, en el año 2019, en su proyecto de investigación, “AUDITORÍA DE SEGURIDAD INFORMÁTICA, RED INTERNA; BASADA EN LA NORMA ISO/IEC 27001; METODOLOGÍA OSSTMMV3”, el autor menciona la importancia de garantizar la confiabilidad, disponibilidad e integridad de la información, por ello aplica una auditoria de seguridad con el fin de hacer un sondeo de la red y detectar vulnerabilidades en la red interna misma que compromete la información que maneja en la institución, además hace uso de la metodología OSSTMM V3 para el análisis en donde propone cambios de medidas de seguridad (Humberto, 2019).

Alexandra Enríquez, en el año 2018, en su proyecto de investigación, “MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA INSTITUCIONES DE SALUD, BASADO EN LAS NORMAS ISO 27799:2008, ISO/IEC 27005:2008 E ISO/IEC 27002:2013 APLICADA A LA CLÍNICA MÉDICA FÉRTIL”, donde el autor propone garantizar la integridad, disponibilidad y la confidencialidad de la información. Mediante la identificación de escenarios en el que la información se ve comprometida ante la inseguridad. El autor concluye en un análisis costo beneficio para la muestra de los controles sobre las políticas que la institución maneja con la finalidad de describir los pasos a seguir para aplicar un

modelo de un Sistema de Gestión de Seguridad de la Información (SGSI) (Alexandra, 2018).

Lema Vinlasaca, en el año 2018, en su proyecto de investigación, “IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013 PARA EL CONTROL FÍSICO Y DIGITAL DE DOCUMENTOS APLICADO A LA EMPRESA LOCKERS S.A.”, el autor propone la implementación de un sistema de gestión de incidencia relacionadas de la seguridad de la información, que contribuyan a establecer políticas y procedimientos que minimicen la materialización de los riesgos en la organización mediante una identificación de las amenazas y vulnerabilidades, priorizar estos riesgos clasificándolos a través de criterios de evaluación (Lema Vinlasaca, 2018).

2.2 FUNDAMENTACIÓN CIENTÍFICA

2.2.1 Gestión de la seguridad de la información

La seguridad de la información esta se refiere a un proceso continuo mismo que está enfocado en:

Garantizar que todos los miembros de la organización reconozcan, evalúen y aborden de manera documentada, metódica, organizada, eficaz y adaptable a los cambios en riesgos y tecnologías, aquellos riesgos asociados con la seguridad de la información. (ISO27000ES, 2013).

Independientemente de su naturaleza o del sector al que pertenezcan, tanto las organizaciones como sus sistemas de información se ven confrontados con un número en constante aumento de amenazas. Estas amenazas tienen el potencial de comprometer los activos críticos de información al aprovechar cualquier vulnerabilidad disponible, lo que los expone a posibles riesgos como fraude, espionaje, sabotaje o vandalismo.

En la actualidad, tanto la información como los procesos y sistemas que dependen de ella han adquirido un papel sumamente relevante como son los activos dentro de cualquier organización.

“La confidencialidad, integridad y disponibilidad de dicha información puede ser fundamental para mantener los niveles de competitividad, conformidad, rentabilidad e imagen de la institución necesarios para conseguir los objetivos de la institución y asegurarse de que haya beneficios económicos” (27000.ES, 2015).

Implementar un modelo de Gestión de Incidentes de Seguridad de la Información mediante la adopción de buenas prácticas, permite utilizar los controles establecidos en la norma ISO/IEC 27002. Esta norma ha sido elaborada con el propósito de ofrecer los requisitos necesarios para establecer, implementar, mantener y mejorar de forma continua un (SGSI) (Chávez, 2021).

2.2.2 Seguridad Informática.

La seguridad informática se enfoca en resguardar el entorno informático, con el objetivo de reducir al mínimo los riesgos que puedan surgir de diversas fuentes, como la entrada de datos, los canales de transporte de la información, el hardware y el personal encargado de los sistemas informáticos (Castro, 2018).

2.2.3 Seguridad de la Información

La seguridad de la información hace referencia a los procedimientos y utilidades diseñados con el propósito de resguardar la información, considerada como un recurso esencial para asegurar la información de una organización (CISCO, 2023).

Por tanto, se puede exponer que la seguridad de la información es una disciplina responsable de proponer y desarrollar estándares, políticas, tecnologías y métodos destinados a realizar sistemas de información seguros y confiables basados en las necesidades del negocio y los valores organizacionales. En la Figura 1, se muestra los aspectos a tomar en cuenta sobre la Seguridad de la Información y la Seguridad Informática.

Figura 1

Seguridad de la Información vs. Seguridad Informática

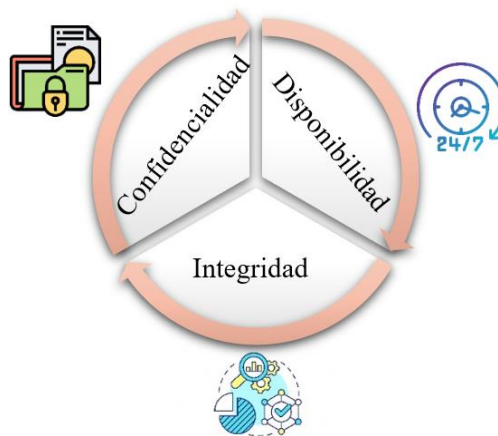


Nota: La figura muestra una comparativa entre dos temas de seguridad que se encuentran relacionados entre sí.

En la Figura 2 se muestra los pilares fundamentales de la seguridad de la información misma que está enfocada en la protección de la información garantizando la confidencialidad, integridad y disponibilidad de los activos de información al aplicar un proceso de gestión de riesgo. De esta manera es importante ejecutar evaluaciones de riesgos para ajustar los procesos para enfrentar una amenaza (Chávez, 2021).

Figura 2

Pilares de la Seguridad de la información



Nota. La figura muestra los tres pilares fundamentales para garantizar la seguridad de la información. Tomado de (ISO27000ES, 2013)

2.2.4 Tipos de Hackers

Hay muchos tipos de piratas informáticos, pero los más comunes y conocidos son los piratas informáticos de sombrero negro, sombrero blanco (Espinoza, 2020).

1. Hacker de Sombrero Negro

Son identificados como hackers que llevan a cabo acciones ilícitas con el propósito de obtener información confidencial de instituciones. Estos atacantes desarrollan programas maliciosos que comprometen la seguridad de las organizaciones sin autorización, con la intención de obtener beneficios personales, frecuentemente de índole económica (Espinoza, 2020).

2. Hacker de Sombrero Blanco

Los hackers de sombrero blanco, también reconocidos como hackers éticos, tienen la responsabilidad de descubrir las vulnerabilidades presentes en un sistema y corregir posibles fallas con el objetivo de fortalecer la seguridad de los sistemas en las organizaciones. (Espinoza, 2020).

3. Hacker de Sombrero Gris

Los hackers de sombrero gris, si bien llevan a cabo actividades ilegales al infiltrarse en la red o servicios de una organización, carecen de intenciones maliciosas. Su objetivo principal es identificar vulnerabilidades en estos sistemas con la intención de informar a la organización correspondiente sobre dichas debilidades. Aunque en algunas ocasiones puedan hacer público el fallo, su intención fundamental es contribuir a la mejora de la seguridad de la empresa (Espinoza, 2020).

2.2.5 Hacking Ético y Pentesting

1. Sistema de Detección de Intrusiones

Un sistema de detección de intrusos (IDS) es un sistema de monitoreo que detecta actividad sospechosa y genera una alerta cuando se detecta (Gashi, 2021).

2. Hacking Ético.

Es una forma de evaluar los servicios que brinda el white hacking, por lo que la empresa se considera una prueba de penetración con el objetivo de analizar si la empresa está bien protegida contra cualquier ataque malicioso

de personas externas que puedan ingresar al sistema de la empresa por medio de la red informática (Academia, 2021).

2.2.6 Metodologías para la evaluación de riesgos.

Como se evidencia en la Tabla 1 y Tabla 2, se hace una comparativa entre las metodologías que más acogida tienen por las organizaciones, donde para la presente investigación se tomó parte del análisis de la metodología MAGERIT que fue desarrollada por el Consejo Superior de Administración del Gobierno de España en 1997.

Magerit permite analizar los riesgos de manera sistemática para valorar la magnitud de los riesgos a los cuales se encuentran expuestos una institución al acceder analizar los riesgos de manera cronológica. Magerit versión 3 es compatible y adaptable a los cambios de la norma ISO/IEC 27002, permitiendo ser una ayuda en términos de organización los mismos que frente a una determinada problemática son flexibles en su desarrollo. (MAGERIT, 2013).

Magerit persigue los siguientes objetivos principales que es enfatizar la metodología para llevar a un correcto análisis de riesgos y que se describen a continuación:

1. Hacer conciencia a los responsables de una institución sobre la importancia de gestionar los riesgos existentes.
2. Realizar un análisis sistemático de los riesgos provenientes del uso de las tecnologías de la información.
3. Colaborar en la detección y tratamiento oportuno de los riesgos identificados para mantenerlos controlados.
4. Preparar a una institución para auditorías, certificación o acreditaciones.

Tabla 1

Metodologías de análisis de riesgos más utilizadas

Característica	MAGERIT	OCTAVE	CRAMM	NIST
----------------	---------	--------	-------	------

Identificación de activos	Separa los activos de la institución en grupos, con la finalidad de identificar riesgos y tomar medidas para prevenir los incidentes.	Considera activos al personal de la misma manera a los sistemas de la institución.	Proporciona un enfoque de activos hardware y software, así como personas.	No dispone de información sobre esta característica.
Valoración de activos	Presenta la caracterización de los valores que representa los activos para la institución, así como las dependencias entre los distintos activos.	No dispone de información sobre esta característica.	La valoración de los activos lo toma como costo reemplazo y en relación al impacto.	No dispone de información sobre esta característica.
Identificación de amenazas	Tiene una relación directa con las amenazas a las que están expuestos los activos informáticos.	Identifica vulnerabilidades tanto tecnológicas como organizativas. Expone a las amenazas creando un riesgo a la organización. Creación de perfiles de amenazas.	Cubre una gran magnitud de problemas potenciales que se usa en grandes organizaciones que puedan afectar a los sistemas de información.	Define amenazas, vulnerabilidades, riesgos y controles. Realiza un análisis de valoración de amenazas e impactos sobre elementos TI. Confidencialidad, disponibilidad, integridad como criterios de seguridad
Identificación de vulnerabilidades	No dispone de información sobre esta característica.	Identifica elementos críticos que son útiles para organizaciones potencialmente de gran magnitud.	No dispone de información sobre esta característica.	No dispone de información sobre esta característica.

Nota. Comparativa entre metodologías de análisis de riesgos más utilizadas. Tomado de (Zambrano, 2019)

Tabla 2

Características de las metodologías de riesgos más utilizadas.

Característica	MAGERIT	OCTAVE	CRAMM	NIST
Recopilación de activos	X		X	X
Identificación de Amenazas	X			
Selección de Salvaguardas	X			
Identificación de vulnerabilidades		X		
Desarrollar planes de seguridad		X		
Comunicar resultados				X

Nota. Tipos de metodologías para obtener una gestión de riesgos, acorde a la organización que se adapte a las necesidades del entorno.

2.2.7 Normas y estándares para la seguridad de la información

En el proceso de gestión de la seguridad de la información, existen varios estándares y buenas prácticas que se pueden llegar a utilizar para crear modelos de gestión de seguridad a nivel de organización. A continuación, se visualiza normas más conocidos y utilizados:

1. BS 7799-3 (British Standards Institution)

Esta norma británica la tercera edición, publicada en 2006, está diseñada específicamente para la gestión de riesgos de seguridad de la información y proporciona una discusión en profundidad sobre la evaluación y gestión de riesgos, incluida la toma de decisiones. La ISO 27001 se considera un

desarrollo adicional de esta norma, que ya cubre la identificación, evaluación, tratamiento y gestión de los riesgos (Unido, 2023).

2. ASHRAE (American Society of Heating, Refrigeration and Airconditioning Engineers)

Responsable de la creación de directrices térmicas, mientras el propósito del estándar ha permanecido invariable – en relación con la especificación de los rangos mínimos de ventilación y otras medidas destinadas a proveer una calidad del aire en entornos de procesamientos de datos (ASHRAE, 2023).

3. BICSI 002-2019 (ANSI/BICSI002)

Mejores prácticas de diseño e implementación cubren todos los sistemas principales que se encuentran dentro de un centro de datos mejores métodos para implementar un diseño que satisfaga sus necesidades específicas (BICSI, 2023).

4. ANSI/TIA-942 (Telecommunications Industry Association)

El Estándar de infraestructura de centros de datos ANSI/TIA-942 es un estándar internacional desarrollado por la Asociación de la industria de las telecomunicaciones (TIA) que define los requisitos y pautas para el diseño de centros de datos. El estándar ANSI/TIA-942 cubre infraestructura de telecomunicaciones, infraestructura eléctrica, infraestructura mecánica, construcción, seguridad contra incendios, seguridad y monitoreo de centros de datos. TIA-942 cubre todo tipo de centros de datos (hiperescala, hosting, empresarial, etc.) (Perkins, 2023).

5. COBIT (Control Objectives for Information Systems and related Technology)

Es un modelo de evaluación y monitoreo que enfatiza en el control de negocios y la seguridad IT y que abarca controles específicos de IT desde una perspectiva de negocios. Las siglas COBIT significan Objetivos de Control para Tecnología de Información y el modelo es el resultado de una investigación con expertos de varios países, desarrollado por ISACA (Information Systems Audit and Control Association) (Villamizar, 2023).

6. COSO - Committee of Sponsoring Organization of the Treadway Commission

COSO es la principal organización que actúa como líder mundial de pensamiento organizacional mediante el desarrollo de marcos y orientaciones generales sobre Control Interno, Gestión de riesgo empresarial y disuasión del fraude dirigidos a mejorar el desempeño organizacional y la supervisión, así como a reducir el nivel de fraude en cualquier organización que lo requiera. (RACINES, 2023)

7. La norma ISO/IEC 20000-1

Es ideal para cualquier proveedor de servicios, grande o pequeño, que quiera garantizar seguridad en la calidad de los servicios que ofrecen. Se usa comúnmente para servicios de TI, administración de instalaciones y servicios comerciales para asegurar que proporcionan unos servicios efectivos en la entrega de servicios de hoy en día. La Norma permite la gestión de servicios de TI de forma metódica a través de la implementación del PHVA (Planear – Hacer – Verificar – Actuar) que ha sido la estructura base y más exitosa de las normas ISO (Charter, 2023).

8. ITIL Information Technology Infrastructure Library

Biblioteca de Infraestructura de Tecnologías de Información define la estructura organizacional y los requisitos de habilidades de una organización de TI y un conjunto de procedimientos y prácticas de gestión operativa estándar para permitir a la organización gestionar una operación de TI y la infraestructura asociada. Los procedimientos y prácticas operativas son independientes del proveedor y se aplican a todos los aspectos dentro de la infraestructura de TI (Filho, 2023).

9. ISO 22301

Es la nueva norma internacional de gestión de continuidad de negocio que, a través del ciclo de mejora continua (PDCA), establece los requisitos para la planificación, el establecimiento, la implantación, la operación, la supervisión, la revisión, la prueba, el mantenimiento y la mejora de un

SGCN documentado teniendo en cuenta la gestión de los riesgos globales de cada organización y su capacidad de resiliencia (AENOR, 2023).

10. UNE 71502:2004

El Sistema de Gestión de Seguridad de la Información ha seguido la metodología Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) versión 2.0. Se está siguiendo el ciclo iterativo PDCA (plan-do-check-act, planificación-implantación-seguimiento-mejora) propugnado por la norma 71502 (MAGERIT, 2013).

11. ISO/IEC 27002

ISO/IEC 27002 es un estándar de seguridad de la información publicado por la Internacional Organization for Standardization derivado de ISO/IEC 27000 que sirve como guía de referencia para las mejores prácticas que incluye las instrucciones para la implementación de seguridad de la información utilizando los pasos que se deben acatar permitiendo a las organizaciones elijan de manera libre los controles que permitan conseguir sus objetivos.

Tabla 3

Comparativa entre las normativas o estándares para seguridad de la información.

NORMA	Características principales	Análisis y gestión de Riesgos	Impacto en la organización	Documentación de aplicabilidad	Controles estándar	Norma predecesora y/o compatible
BS77993	- Se vincula con la toma de decisiones con la Dirección. - Diseñada específicamente para la gestión de riesgos de seguridad de la información.	SI	SI	NO	NO	27001

ASHRAE	<ul style="list-style-type: none"> - Responsable de la creación de directrices térmicas. - Creación de directrices para el entorno del centro de datos. 	NO	NO	SI	NO	----
BICSI002	<ul style="list-style-type: none"> - Mejores prácticas de diseño e implementación cubren todos los sistemas principales que se encuentran dentro de un centro de datos. - Cubre los factores fundamentales para la implantación y diseño de un centro de datos. 	NO	NO	SI	NO	----
ANSI/TIA-942	<ul style="list-style-type: none"> - Enfocada en las mejores prácticas para la infraestructura de un centro de datos. - Cubre infraestructura de telecomunicaciones, construcción, seguridad contra incendios, seguridad y monitoreo de centros de datos. 	NO	NO	SI	NO	----

COBIT	<ul style="list-style-type: none"> - Orientada a clarificar cuestiones actuales y futuras en cuanto, a administración, - Seguridad y aseguramiento de tecnologías de información. - Modelo de evaluación y monitoreo en TI. 	NO	SI	SI	SI	27002 y C
COSO	<ul style="list-style-type: none"> - Definición de controles internos, normas y criterios para evaluar sistemas de control. - Desarrollo de marcos y orientaciones generales sobre Control Interno, Gestión de riesgo empresarial. 	NO	SI	SI	NO	COBIT y
ISO/IEC 20000	<ul style="list-style-type: none"> - Indica las mejores prácticas para la gestión de Servicios en TI. - Permite la gestión de servicios de TI de forma metódica a través de la implementación del PHVA 	SI	NO	SI	NO	Proviene de BS15000 evolucionada a ISO/IEC 27013
ITIL	<ul style="list-style-type: none"> - Las mejores prácticas en la Gestión de Servicios TI, incluyendo opciones para la adaptación según las necesidades del proveedor de servicios. - Los procedimientos y prácticas operativas son independientes del proveedor y se aplican a todos los aspectos dentro de la infraestructura de TI. 	NO	NO	SI	SI, para el ciclo de vida de los servicios	Integrada con ISO/IEC 20000
ISO 22301	<ul style="list-style-type: none"> - Buenas prácticas para la gestión de continuidad de negocio. - La nueva norma internacional de gestión de continuidad de negocio que, a través del ciclo de mejora continua (PDCA). 	SI	SI	SI	SI	Sustituida por la integrada ISO/IEC 27001

<p>UNE 71502:2004</p>	<p>- Especifica los requisitos para establecer, implementar, documentar y evaluar un SGSI en el contexto de los riesgos organizacionales.</p>	<p>SI</p>	<p>SI</p>	<p>SI</p>	<p>SI</p>	<p>Cortada vigencia por publicación de la ISO/IEC 27001</p>
<p>ISO/IEC 27002</p>	<p>- Se está siguiendo el ciclo iterativo PDCA. - Define los requisitos para la creación, implementación, documentación y evaluación de SGSI en el contexto de riesgos organizacionales, con base en un enfoque de procesos y mejora continua. - Montar los componentes del SGSI, incluidas las piezas documentadas para su gestión y mantenimiento; la definición de controles de seguridad comienza con el Apéndice A y finaliza con la revisión y mejora del SGIS</p>	<p>SI</p>	<p>SI</p>	<p>SI</p>	<p>SI</p>	<p>Compatibilizada con COBAC y COSO. ISO/IEC 27000, IT ISO22301</p>

Nota. Comparativa entre once de las normativas o estándares más destacados para la seguridad de la información. Tomado de varios autores ((Unido, 2023); (ASHRAE, 2023); (BICSI, 2023); (Perkins, 2023); (Villamizar, 2023); (RACINES, 2023); (Charter, 2023); (Filho, 2023); (AENOR, 2023); (MAGERIT, 2013); (ISO27000ES, 2013)).

Con base en el análisis de diversos estándares internacionales de seguridad de la información, mostrado en la Tabla 3, se puede mencionar que el estándar que mejor se adaptó a las necesidades de gestión de la información a nivel organizacional es el estándar ISO/IEC 27002, ya que cubre las mejores prácticas que ofrecen sus estándares anteriores. Esta norma es en definitiva una herramienta muy útil para quienes sean los responsables de iniciar, implantar o mantener la seguridad de una organización, la ISO/IEC 27002 no es una norma de certificación, ni fue diseñada para ese propósito, la misma es seguida por la norma ISO/IEC 27001 la cual define los requisitos necesarios para implementar y gestionar un SGSI y es un estándar certificable.

2.2.8 Estándares que componen la Familia de la Norma ISO/IEC 2700

La Organización Internacional de Normalización ISO (International Organization for Standardization), es una organización que se especializa en la difusión de los estándares y la Comisión Electrotécnica Internacional IEC (International Electrotechnical Commission) ambas conforman un sistema especializado de normalización a nivel mundial. Los organismos ISO y la IEC, y los recursos que están involucrados para ello dependerán, del nivel de actividad ejercida, ambas colaboran de manera conjunta para la elaboración de las normas internacionales (ISO, 2022).

Norma ISO/IEC 27000 Los estándares que componen la familia ISO/IEC-27000 son un conjunto de estándares creados y administrados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrónica Internacional (IEC). Ambas organizaciones internacionales cuentan con una amplia distribución, implementación y reconocimiento en todo el mundo. Facilita las bases y lenguaje común para el resto de las normas de la serie (ISO, 2022). Se describe a continuación en la Tabla 4 una descripción resumida de las normas pertenecientes a la familia 27000.

Tabla 4

Normas Técnicas pertenecientes a la familia 27000

NORMA	Descripción
ISO 27000	Presenta los conceptos básicos de seguridad de la información, el vocabulario y describe el SGSI en una visión de conjunto.
ISO 27001	Define los requisitos necesarios para implementar y gestionar un SGSI. El estándar es certificable.
ISO/IEC 27002	Define un conjunto de buenas prácticas para la implementación del SGSI utilizando 114 controles agrupados en 14 áreas y 35 objetivos de control.
ISO 27003	Proporciona orientación para la implementación adecuada del SGSI, centrándose en los aspectos críticos de la implementación exitosa.

ISO 27004	Proporciona orientación sobre cómo definir y crear correctamente métricas para medir correctamente el rendimiento del SGSI.
ISO 27005	Cómo se debe realizar la gestión de riesgos en relación con los sistemas de gestión de la información, centrándose en la metodología a utilizar.
ISO 27006	Defina los requisitos para las organizaciones que buscan la certificación para demostrar el cumplimiento de ISO/IEC-27001.
ISO 27007	Es una guía para establecer procedimientos de auditoría interna o externa para verificar y certificar la implementación de ISO/IEC-27001.
ISO 27008	Definir cómo se deben evaluar los controles del SGSI para revisar su adecuación técnica para mitigar los riesgos de manera efectiva.
ISO 27009	Complementa el estándar 27001 con requisitos específicos de la industria y nuevos controles diseñados.
ISO 27010	Especifica cómo se debe manejar la información cuando se comparte entre varias organizaciones, qué riesgos pueden surgir y los controles que se deben usar para mitigar esos riesgos, particularmente en relación con la gestión de seguridad de la infraestructura crítica.
ISO 27011	Define los principios para implementar, mantener y administrar un SGSI en una organización de telecomunicaciones y muestra cómo se pueden implementar controles de manera efectiva Norma ISO/IEC 27002.
ISO 27013	Cree una guía para las organizaciones que implementan los estándares de ISO/IEC 27001 e ISO/IEC 270000-1.
ISO 27014	Establece los principios de la gestión de la seguridad de la información para que las organizaciones puedan evaluar, monitorear y comunicar las actividades relacionadas con la seguridad de la información.
ISO 27015	Ayuda a implementar los principios del SGSI en empresas que brindan servicios financieros, como bancos o banca electrónica.
ISO 27016	Proporciona orientación sobre la toma de decisiones financieras relacionadas con la gestión de la seguridad de la información como ayuda para la gestión de la organización.
ISO 27017	Brinda orientación sobre 37 controles específicos para servicios en la nube basados en el estándar 27002.

ISO 27018	Complementa los estándares 27001 y 27002 al implementar procedimientos y controles para proteger los datos personales en las organizaciones que brindan servicios en la nube a terceros.
ISO 27019	Proporciona orientación basada en el estándar 27002 para industrias relacionadas con la energía para implementar un SGSI.
ISO 27031	Directrices para la continuidad del negocio de la TIC.
ISO 27799	Gestión de SI en sanidad utilizando la Norma ISO/IEC 27002.

Nota. Normas técnicas importantes dentro de la familia ISO/IEC 27000 a partir de (Alonso, 2023)

ISO/IEC 27002

El estándar ISO/IEC 27002 tiene un total de 14 controles de seguridad de la información o dominios con 35 objetivos de control, que brindan un detalle claro del total de 114 controles de seguridad que son opcionales y deben ser analizados para su desarrollo e implementación en una determinada institución, por lo que se deben tener en cuenta para lograr los objetivos del SGSI.

De esta manera, en el caso de ocurrir un incidente, se pueden minimizar las pérdidas y garantizar la continuidad del negocio. En segundo lugar, la racionalización de recursos puede conducir a ahorros de costos. A continuación, en la Figura 3 se muestra el contenido de la Norma ISO/IEC 27002:2013.

Figura 3

Contenidos clave de la norma ISO/IEC 27002:2013



Nota. Elementos clave para tener en cuenta en la seguridad de la información. Tomado del Instituto Uruguayo de Normas (Técnicas, 2015)

Los controles de la ISO/IEC 27002, contienen un enfoque específico, que apoya en el proceso de conseguir y llevar a cabo un modelo de gestión de seguridad informático propuesto la presente investigación, tiene buenas prácticas orientadas a procesos y sigue el modelo del ciclo PDCA.

Para mitigar un riesgo, es necesario abordar las vulnerabilidades identificadas mediante la implementación de controles. Estos mecanismos, una vez aplicados, logran disminuir el riesgo a un valor mínimo, el cual la dirección debe evaluar nuevamente para determinar si es aceptable o si es necesario seguir mejorando los controles.

Es importante destacar que los controles influyen en las amenazas al reducir tanto la degradación como la probabilidad asociadas a ellas. En la Figura 4 se puede observar la estructura de los catorce controles de la norma ISO/IEC 27002.

Figura 4

Estructura de Controles de ISO/IEC 27002



Nota. Esta figura muestra los catorce controles desplegados, que conforman los controles de la norma ISO/IEC 27002 (ISO27000ES, 2013)

Buenas prácticas establecidas por la NORMA ISO/IEC 27002

La norma ISO/IEC 27002 proporciona un conjunto de pautas que detallan los aspectos clave de ISO 27001. Combinados, estos dos estándares abarcan todas las áreas concebibles

de seguridad y protección de la información. Esta norma es aplicable a organizaciones de cualquier índole, ya sean del ámbito comercial o público, y establece sistemas de seguridad de la información para validar los procedimientos de diseño en la gestión de la protección de activos informáticos. Las mejores prácticas definidas por la norma ISO/IEC 27002 son:

5. POLITICAS DE SEGURIDAD.

5.1 Directrices de la Dirección en seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.

6.1 Organización interna.

6.2 Dispositivos para movilidad y teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

7.1 Antes de la contratación.

7.2 Durante la contratación.

7.3 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.

8.1 Responsabilidad sobre los activos.

8.2 Clasificación de la información.

8.3 Manejo de los soportes de almacenamiento.

9. CONTROL DE ACCESOS.

9.1 Requisitos de negocio para el control de accesos.

9.2 Gestión de acceso de usuario.

9.3 Responsabilidades del usuario.

9.4 Control de acceso a sistemas y aplicaciones.

10. CIFRADO.

10.1 Controles criptográficos.

11. SEGURIDAD FÍSICA Y AMBIENTAL.

11.1 Áreas seguras.

11.2 Seguridad de los equipos.

12. SEGURIDAD EN LA OPERATIVA.

12.1 Responsabilidades y procedimientos de operación.

12.2 Protección contra código malicioso.

12.3 Copias de seguridad.

- 12.4 Registro de actividad y supervisión.
- 12.5 Control del software en explotación.
- 12.6 Gestión de la vulnerabilidad técnica.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
- 13. SEGURIDAD EN LAS TELECOMUNICACIONES.**
 - 13.1 Gestión de la seguridad en las redes.
 - 13.2 Intercambio de información con partes externas.
- 14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.**
 - 14.1 Requisitos de seguridad de los sistemas de información.
 - 14.2 Seguridad en los procesos de desarrollo y soporte.
 - 14.3 Datos de prueba.
- 15. RELACIONES CON SUMINISTRADORES.**
 - 15.1 Seguridad de la información en las relaciones con suministradores.
 - 15.2 Gestión de la prestación del servicio por suministradores.
- 16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.**
 - 16.1 Gestión de incidentes de seguridad de la información y mejoras.
- 17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.**
 - 17.1 Continuidad de la seguridad de la información.
 - 17.2 Redundancias.
- 18. CUMPLIMIENTO.**
 - 18.1 Cumplimiento de los requisitos legales y contractuales.
 - 18.2 Revisiones de la seguridad de la información.

CAPITULO III

MARCO METODOLÓGICO

3.1. Tipo de investigación

La presente investigación acorde a la necesidad planteada en la Administración de Redes de la FISEI de la UTA es de tipo cualitativa y aplicada, fundamenta en conocer las actividades, procedimientos los cuáles son las vulnerabilidades que afectan actualmente a dicha organización.

Investigación Cualitativa

Desempeña un papel esencial en el ámbito de la seguridad de la información al permitir una comprensión en profundidad de los factores que influyen en la gestión y protección de los datos sensibles. La investigación cualitativa no solo contribuye a mejorar las estrategias de protección de la información, sino que también fomenta una conciencia más profunda sobre la importancia de la seguridad informática en un entorno cada vez más digitalizado e interconectado.

Investigación Bibliográfica

Se aplica este tipo de investigación porque se centra en encontrar fundamentación teórica, artículos científicos, el cual permita elaborar un correcto marco teórico vasto.

Investigación de Campo

Se recolecta información primaria en base a una entrevista con el personal a cargo del departamento de Administración de Redes de la FISEI, adicionalmente se hace un análisis de vulnerabilidades a través de herramientas.

3.2. Población o muestra

El presente trabajo de investigación se llevó a cabo en la Universidad Técnica de Ambato para la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, en el Bloque 1 de la facultad posee sitios clave donde se encuentran los racks que alojan switches de capa dos y tres, la central de voz IP, dos equipos DVR, cámaras distribuidas en el bloque, en la red se despliega APS ubicados en sitios estratégicos.

En el Bloque 2 de la facultad se encuentra un rack que aloja switches de capa dos, cámaras distribuidas en el bloque.

No obstante, dado a la confidencialidad de los datos no se divulgará la información, se detalla que las actividades se están realizadas únicamente sobre los activos y sistemas siguientes:

- Infraestructura física de la FISEI.
- Redes de datos.
- Servidor de Aplicativos y equipos de almacenamiento.
- Sistema de cámaras de seguridad NVR Hikvision.

Para el desarrollo de recopilación de información de datos se lo realizará haciendo uso de técnicas como entrevistas y observación directa, recopilando de esta manera información valida y actual que permita ejecutar al análisis de la seguridad de la información que se detallará en el desarrollo de esta investigación.

3.3. Recolección de información

Como primera instancia se realizó una recopilación de información basado en trabajos de investigación, artículos científicos, tesis del repositorio de la Universidad Técnica de Ambato y de diferentes universidades que se alineen al proyecto.

Para recopilar información, se han realizado entrevistas al personal encargado de la Administración de Redes de la FISEI, para identificar casos en donde no se aplicaron controles o procedimientos relacionados con los activos de seguridad de la información y para evaluar si la información que están utilizando actualmente es consistente con las políticas de seguridad de la institución y a su vez la utilización de políticas de seguridad de la información relacionados con el tema propuesto, cuyo fin es brindar información básica para el presente proyecto de investigación.

Para las entrevistas se utilizó un cuestionario de evaluación elaborado según los controles de la norma ISO/IEC 27002 dirigida al departamento de Administración de Redes de la FISEI, con el fin de conocer las actividades que se realizan normalmente para no perder información relevante para el desarrollo de la investigación.

Además, se realizó observaciones de campo, ya que es importante conocer los activos informáticos necesarios para comprender la arquitectura de red y los equipos informáticos propiedad de la institución, para posteriormente proceder con la verificación del desempeño de la seguridad de la información garantizando su correcto uso.

3.4. Procesamiento de la información.

Para llevar a cabo el proyecto de investigación se realiza un orden cronológico y de esta manera llegar a cumplir los objetivos planteados, los pasos a seguir son los siguientes:

1. Realizar una búsqueda de información en sitios de fuentes confiables.
2. Desarrollar las entrevistas en base a la norma ISO/IEC 27002.
3. Evaluación de herramientas para la identificación de vulnerabilidades.
4. Análisis de la información conseguida con relación a los lineamientos de proyecto de investigación planteado.
5. Exponer y explicar los resultados obtenidos.

CAPITULO IV

RESULTADOS Y DISCUSIÓN

4.1 Estado inicial de la institución

Con el objetivo de conocer el estado inicial del área de Administración Redes de la FISEI, se parte de las entrevistas realizadas al personal responsable, respecto al tema de la seguridad de la información, permitiendo conocer los procesos internos y políticas que maneja dicho departamento.

Posteriormente es importante realizar un análisis de la entrevista misma que será punto de partida para desarrollar una gestión adecuada, considerando que se debe hacer énfasis en los aspectos negativos considerando como punto de vista el buen manejo de la seguridad de la información.

La entrevista en mención se la realizo al Analista de TICs (Tecnologías de la información y comunicación), misma que tiene una larga trayectoria desempeñando sus labores en la FISEI aproximadamente 12 años, de la misma manera se la realizo al Docente encargado de la Comisión de Laboratorios que lleva 7 meses a cargo de la gestión del departamento antes mencionado.

Estas entrevistas fueron realizadas previas al desarrollo del proyecto de investigación, mediante esta información adquirida en estas entrevistas, se pudo llegar a un diagnóstico el cual influencio en la toma de decisiones para llegar a la justificación del presente proyecto de investigación. Con esto se pudo comprobar que el departamento de Administración Redes de la FISEI, presenta una problemática con relación a la gestión de seguridad para el manejo adecuado de la información crítica para la institución.

A continuación, en la Tabla 5, se puede apreciar las respuestas de los responsables del área de Administración Redes de la FISEI, donde se obtuvieron las siguientes respuestas del personal a cargo:

Tabla 5

Resultados de la entrevista al personal experto del Departamento de Administración de Redes de la FISEI.

Entrevistado/a	Respuesta SI/NO	Respuesta SI/NO	
----------------	-----------------	-----------------	--

Pregunta	Analista de TICs	Docente Comisión de Laboratorios	
Políticas de seguridad de la información			
¿El departamento de Administración de Redes cuenta con políticas de seguridad de la información?	Si. Existen políticas de seguridad que cubren parte de la Administración de Redes, pero son generales a nivel de la UTA.	No. Existen políticas internas las mismas que se encuentran desactualizadas y no están acorde al crecimiento que va teniendo la institución.	Se p cuer info Adm enci
¿El personal técnico y administrativo de la UTA FISEI tiene conocimiento de las políticas de seguridad de la información?	Si. El personal cuenta con el conocimiento y el material a la mano de las políticas existentes, las cuales se entregaron al iniciar su contratación en la institución.	Si. El personal tiene el conocimiento de las políticas existentes a nivel de la UTA y a nivel de facultad.	El poli inst
¿Se ha implementado los controles de cumplimiento acerca de las políticas de seguridad de la información?	No. La implementación de políticas de seguridad de la información no se tiene implementado.	No. Existen políticas internas, pero no están enfocadas a la seguridad de la información.	Emp segu se e
¿Se cuenta con políticas de seguridad que se encarguen de supervisar la manera en la que se manipula la información?	Si. Existen políticas que definen la responsabilidad de la información al propio personal de custodiar su información y la que vaya generando.	Si. La manipulación y cuidado de la información se encentra parcialmente asignado a cada personal.	Es i info resp
¿Los incidentes de seguridad de los sistemas de información son reportados brevemente por el personal?	No. Dado a la falta de capacitación al personal que genera información, al suceder algún tipo de incidente no se reporta a la brevedad necesaria.	No, Falta de capacitaciones al personal en caso de suceder incidentes de seguridad.	Se p al p pos info
Aspectos organizativos para la seguridad			
¿La FISEI cuenta con un área para uso exclusivo del desempeño de la seguridad de la información?	No. La falta de espacio y organización en la institución no ha permitido diseñar un área exclusiva para este tipo de seguridad.	No. Dado a que se debe destinar un área exclusiva y no se hecho la gestión adecuada para brindar la importancia al tema de seguridad.	Se p asig segu añor

¿La FISEI ha contratado un asesoramiento en materia de seguridad de la información?	No. Acorde a las políticas de seguridad de la información de la institución no se ha visto tan necesario contratar asesoramiento externo.	No. Se ha evidenciado que no es tan importante contratar asesoramiento externo por la poca afluencia de datos críticos en la institución.	Se p mar críti tien
¿Al realizar contratos con empresas externas exige cláusulas de seguridad de la información?	No. Se ha contratado empresas externas para la seguridad de la información.	No. Se ha contratado empresas externas para la seguridad de la información.	Con segu
¿En el caso de migrar al teletrabajo, se cuenta con herramientas actualizadas y plataformas educativas para continuar con normalidad?	Si. La institución tiene plataformas actualizadas para migrar al tema de teletrabajo.	Si. La institución cuenta con la capacitación y el software necesario para migrar al teletrabajo por cualquier circunstancia.	Se p plat deb tem mar

Con relación a la gestión de activos informáticos

¿Se cuenta con un inventario de activos de información actualizado?	Si. La facultad cuenta con un departamento de bienes que se encarga de actualizar los activos.	Si. Se dispone de un departamento de bienes que tiene actualizado los activos.	Mar inst acti
¿El inventario esta automatizado?	No. Falta de contratación de empresas para generar automatización de inventario. Tiene vinculado con página del Gobierno.	No. El inventario tiene su sistema mediante una plataforma del Gobierno.	Se p vinc deb de a
¿El inventario de los activos informáticos es actualizado de manera periódica?	Si. El personal encargado del inventario de los activos se encuentra pendiente de actualizar de manera periódica.	Si. Se cuenta con una actualización periódica de activos en la institución.	Se c acti actu
¿Los activos informáticos se encuentran correctamente etiquetados?	Si. Todos los activos que ingresan a la institución se encuentran correctamente etiquetados e identificados.	Si. Todos los activos que se reciben en la institución son etiquetados.	El p en e

Con relación al control de acceso

¿En cuanto a las aplicaciones en la relación a las usadas en la FISEI, cuentan con	No. Las aplicaciones usadas tienen políticas de control de acceso documentadas.	No. Falta de documentación en cuanto a políticas de seguridad.	Se usac poli
--	---	--	--------------------

políticas de control de acceso?			
¿Se cuenta con un control de acceso a las redes y servicios asociados?	No. Políticas asociadas a las redes y demás servicios en la institución no se encuentra documentado.	No. Falta de políticas de control de acceso a las redes de la institución.	En l con con
¿Se cuenta con procedimientos seguros para el inicio de sesión con relación al personal docente y área administrativa?	No. Falta de implementar medidas de seguridad en las aplicaciones y procedimientos seguros en relación al inicio de sesión.	No. Falta de procedimientos seguros en cuanto al inicio de sesión en aplicaciones utilizadas en la institución.	Se p proc sesi
¿Todas las aplicaciones de la FISEI cuentan con una contraseña para permitir el acceso a los usuarios?	No. Existen aplicaciones que no precinden de contraseñas y están disponibles para el uso común y son de carácter informativo.	No. Aplicaciones que son de carácter informativo no tienen contraseñas solo se acceden con escaneo de códigos QR.	Se e brec acce
¿Para el acceso remoto se tiene establecidos mecanismos de autenticación de usuarios para el acceso a la red interna de la institución?	No. La institución no cuenta con mecanismos para uso de acceso remoto o aplicaciones que permitan el ingreso. Se cuenta con un VPN usado para servicios de Quipux.	No. El único acceso que se dispone es de una aplicación llamada FortiClient que permite acceder a servicios como Quipux institucional.	Se apli uso doc
¿Las políticas de control de acceso son aplicadas?	No. Falta de políticas de control de acceso documentadas.	No. Falta de políticas de control de acceso documentadas.	Se desa imp
¿Cuentan con un inventario actualizado para los accesos otorgados a los sistemas informáticos?	No. Falta de documentación en la otorgación de permisos y accesos a los sistemas informáticos.	No se dispone de un inventario documentado de la otorgación de accesos a los sistemas informáticos.	Se p info siste

Con relación al cifrado

¿Para el uso y almacenamiento de la información por parte del personal de la institución cuenta con políticas de controles criptográficos?	No se cuenta con políticas de seguridad criptográfico en las aplicaciones utilizadas en la institución.	No se dispone de controles criptográficos en la institución.	Se p crip
--	---	--	--------------

¿Se gestiona las claves de manera segura de cada uno de las áreas y departamentos de la FISEI?	No se encuentra documentada de manera segura las claves de acceso a las áreas de la institución.	No. Hace falta documentar las claves de cada área de los departamentos de la institución.	Se doc
¿Se cuenta con un procedimiento de control de los cambios para las aplicaciones, software y sistema operativo?	No. Los cambios en las aplicaciones no cuentan con procedimientos documentados.	No los cambios se los hace de acuerdo a los requerimientos y según se vayan requiriendo, pero no se documenta.	Se proc doc
¿Se validan los códigos fuentes desarrollados por personal externo antes de la puesta en producción?	No se adquiere aplicaciones desarrolladas por empresas externas.	No se adquiere aplicaciones desarrolladas por empresas externas.	No real emp

Con relación a la seguridad física y ambiental

¿La FISEI cuenta con un procedimiento formal para reportes de incidentes?	No se dispone de reportes de incidentes que se documente.	No se lleva la documentación de reportes de incidentes en la institución.	Se doc
¿Cuentan con una herramienta de registro de incidentes o Help desk?	No se dispone de herramientas para registro de incidentes.	No registro netamente de accidentes, no se lleva un registro.	Se regi inci
¿Al reportar un incidente de seguridad se cuenta con un plan de respuesta?	No. Se lleva reportes de incidentes, pero en dificultades se da respuesta a la brevedad posible.	No se cuenta con un plan de respuesta que permita dar una solución más rápida.	Se p dar de r
¿Se investiga y recolectan evidencias sobre el incidente de seguridad?	No se ha llevado un registro ni historiales de incidentes de seguridad.	No se cuenta con una documentación ni tampoco se hace investigaciones sobre algún incidente sucedido.	Se p no inci
¿Todas las áreas se encuentran correctamente identificadas?	Si. Todas las áreas en la institución cuentan con su respectiva identificación.	Si las identificaciones en la institución se encuentran correctamente actualizadas.	Se p cuer
¿Para acceder a las áreas seguras se cuenta con los respectivos controles y	No para el ingreso a las áreas seguras falta documentar controles de restricciones y señalética correspondiente.	No hace falta colocar la respectiva información de restricción a cada área.	Se p hac pers doc

restricciones de ingreso del personal no autorizado?			
¿En caso de alguna falla en los equipos informáticos se está preparados para su pronta corrección?	Si se cuenta con el personal capacitado para dar solución de manera inmediata a cualquier falla.	Si en caso de fallar algún tipo de equipo informático se cuenta con el personal capacitado.	Se cuenta con el personal capacitado para dar solución de manera inmediata a cualquier falla.
¿Se realiza mantenimiento periódico al hardware y software a los equipos informáticos de la institución?	Si la actualización se la realiza cada 6 meses al finalizar el ciclo académico.	Si se realiza mantenimientos periódicos de la misma manera se lleva fichas técnicas con su registro.	Se realiza mantenimiento periódico al hardware y software a los equipos informáticos de la institución.

Administración de la continuidad de los sistemas Informáticos

¿La FISEI cuenta con planes de continuidad de las operaciones?	No se tiene planes de continuidad de operaciones.	No cuenta con planes de continuidad en las operaciones.	Se cuenta con planes de continuidad de las operaciones.
¿Realizan pruebas, mantenimiento y evaluación constante de los planes de continuidad de las operaciones?	No se tiene planes de continuidad de operaciones.	No cuenta con planes de continuidad en las operaciones.	Se realizan pruebas, mantenimiento y evaluación constante de los planes de continuidad de las operaciones.

Con relación a la seguridad en la operativa

¿Se realiza periódicamente copias de seguridad de la información (backups)?	No se cuenta con backups de seguridad.	No se cuenta con backups de seguridad.	Se realiza periódicamente copias de seguridad de la información (backups).
¿Se lleva un control correspondiente a la gestión de las vulnerabilidades técnicas?	No se lleva una gestión de vulnerabilidades técnicas, y tampoco un control.	No se tiene controles en la gestión de vulnerabilidades, falta de identificación de las mismas.	Se lleva un control correspondiente a la gestión de las vulnerabilidades técnicas.
¿Se cuenta con restricciones en la instalación de software?	Si tanto laboratorios como personal tanto docentes como administrativos tienen restricciones en la instalación de software.	Si se cuenta con restricciones mediante claves de administrador que no les permite instalación de software.	Se cuenta con restricciones en la instalación de software.

¿Se realiza controles de auditoría de los sistemas de información?	No se realiza controles de auditoría a nivel de facultad, pero periódicamente la Universidad hace auditorías internas y hace visitas verificando activos.	No cuenta con los controles de auditoría a nivel de facultad.	Se p con sob siste
--	---	---	-----------------------------

Nota. Esta tabla muestra los resultados del criterio experto del personal a cargo del departamento de Administración de Redes de la FISEI.

Interpretación de Resultados de las entrevistas recopiladas

Por medio de la información adquirida en las entrevistas con el personal experto del departamento de Administración de Redes de la FISEI, proporciona una visión integral de las percepciones basadas en la experiencia de los participantes en la encuesta. Por lo que se procede a usar herramientas para una mejor identificación de las vulnerabilidades encontradas en los activos informáticos de la FISEI.

- Con base a los resultados obtenidos en las entrevistas se puede evidenciar que el departamento de Administración de Redes se encuentra vulnerable a riesgos informáticos que pueden llegar a dañar el buen funcionamiento de la institución.
- Existen políticas de seguridad de la información a nivel de la UTA, pero ante alguna eventualidad estas políticas no se adaptan a la realidad de una estructura organizacional que genera su propia información y mantiene sus procesos internos.
- Se puede evidenciar que la FISEI cuenta con un debido proceso a través del personal de administración de bienes, cuya función en especial es etiquetar tanto los bienes inmuebles como tecnológicos y mantenerlos actualizados.
- En la FISEI existen plataformas móviles las cuales no cuentan con mecanismos de seguridad de inicio de sesión, mismos que pueden ser un problema de seguridad. Informático.
- Se puede evidenciar que la FISEI cuenta con claves de autenticación para el acceso a la red interna de la UTA mediante una aplicación llamada FortiClient para acceder a sus respectivos servicios.
- En cuanto al uso del almacenamiento de la información el personal no cuenta con los controles sobre políticas de seguridad criptográficas que ayuden a mantener seguro los datos.
- Al suscitar algún tipo de incidente, la institución no cuenta con una herramienta que registre el tipo de inconveniente existió para en futuras situación se logre solucionar de mejor manera.

- La FISEI no cuenta con una pronta respuesta ante una correcta continuidad de operaciones la misma que debería de ser principal característica ante una institución que debe funcionar a la brevedad posible.
- Periódicamente la institución debería llevar un respaldo de la información que genera cada dependencia en especial las distintas coordinaciones existentes, toda esta información no cuenta con backups.
- En cuanto a tener un control de auditorías de los sistemas de información a nivel de facultad no se lo realiza, a nivel de Universidad cuentan con una visita a las facultades haciendo constatación de activos y revisión de documentación actualizada.

4.2 Gestión de la Seguridad de la Información

Para ejecutar el análisis y la evaluación del estado actual de la seguridad de la información en la institución se utilizan una serie de herramientas informáticas para examinar las vulnerabilidades en puertos, infraestructuras y servicios, los detalles sobre estas herramientas son los siguientes:

Detección de vulnerabilidades y monitoreo de puertos

El análisis del sondeo de puertos es importante por lo que se hace una comparativa entre algunas herramientas como se puede apreciar a continuación en la Tabla 6.

Tabla 6

Herramientas populares de sondeo de puertos en una determinada red.

Herramienta	Nmap	SuperScan4	NetScan6	Advanced Port Scanner
Característica				
Escaneo de puertos	SI	SI	SI	SI
Plataforma	Windows Mac Linux Unix	Windows	Windows	Windows y Linux
Escaneo de vulnerabilidades	SI	NO	NO	NO
Licencia	Libre	Libre y Pagado	Libre y Pagado	Libre
Documentación	Amplia	Limitada	Limitada	Amplia
Funciones	Análisis de puertos abiertos y monitorización de redes, servidores, aplicaciones ejecutándose.	Análisis de Puertos TCP, Pruebas de ping a direcciones IP.	Análisis de Puertos NetBIOS Direcciones IP, direcciones MAC.	Permite realizar un análisis al encontrar con rapidez todos los puertos abiertos (TCP y UDP)
Uso	Mapear una red, Identificar servicios en ejecución, Realizar una auditoría de seguridad, Detectar sistemas operativos.	Monitoreo y control de host y dominios, evaluación de la seguridad de la red de computadores.	Administración de la red, recopilación de información.	Exploración rápida de los dispositivos de la red. Fácil acceso a los recursos encontrados: HTTP, HTTPS, FTP, carpetas compartidas.

Nota. En la tabla muestra populares herramientas de sondeo de puertos informáticos.

De acuerdo con las características de las herramientas descritas en la Tabla 6, Nmap es una buena opción y la que mejor se adapta a las necesidades del departamento de Administración de Redes de la FISEI, como es detección de servidores, puertos abiertos, aplicaciones que se encuentren en ejecución, servicios, identificación de la versión del

sistema operativo, DNS, direcciones MAC, así mismo cuenta con soporta direcciones IPv4 e IPv6.

Para el análisis de vulnerabilidades se hace una comparativa en la Tabla 7, en aplicaciones que se acceden en la web se realiza un estudio de las herramientas más utilizadas a continuación:

Tabla 7

Herramientas de detección de vulnerabilidades.

Herramienta	IBM Security QRadar	Nessus	OpenVAS
Característica			
Escaneo de vulnerabilidades	<ul style="list-style-type: none"> • Identifica vulnerabilidades en aplicaciones web. • Análisis para detectar amenazas en la red y en equipos. • Dispone de alerta de seguridad. • Analiza datos de registro de varios dispositivos. • Realiza un monitoreo y visibilidad sobre una amenaza potencial. 	<ul style="list-style-type: none"> • Realiza una búsqueda de vulnerabilidades en el host y aplicaciones web. • Detección de Recursos. • Escaneo de redes. • Evaluación de riesgos. • Controles, configuración y permisos de acceso. 	<ul style="list-style-type: none"> • Identifica vulnerabilidades en aplicaciones web proporcionando una guía de solución para mejorar la seguridad. • Servidor web integrado. • Escaneo concurrente de múltiples nodos. • Escaneo automático temporizado.
Plataformas	Windows	Multiplataforma	Multiplataforma
Licencia	Pagado	Libre y pagado	Libre
Reportes	No dispone de la parte de reportes.	Genera informes detallados en formatos (PDF, CSV, XML, HTML),	Genera informes detallados sobre los formatos (XML, HTML, LaTeX, entre otros).

Soporte Técnico	Cuenta con actualizaciones disponibles.	Cuenta con actualizaciones disponibles.	Cuenta con actualizaciones disponibles.
-----------------	---	---	---

Nota. Esta tabla muestra las características principales de cada herramienta de detección de vulnerabilidades.

De acuerdo al análisis de la Tabla 7, se puede apreciar que la herramienta Nessus una buena opción si la cantidad de equipos a escanear es menor a 16 caso contrario se debería adquirir una licencia. Entre sus principales características destacan un fácil y completo análisis para buscar vulnerabilidades en una determinada organización

Se puede realizar escaneos detallados y analizar múltiples computadoras al mismo instante, y una vez finalizado el análisis se puede obtener un reporte completo de la cantidad de vulnerabilidades, y para un mejor entendimiento y toma de decisiones rápido la herramienta muestra resultados con códigos de colores que den alertas del resultado del análisis.

También cuenta con escaneo automático, avanzado y personalizado, análisis de vulnerabilidades, análisis de páginas web, escaneo de redes, control, configuración y permisos de acceso, y detección de recursos, evaluaciones de riesgos y también cuentan con informes fáciles de interpretar en una variedad de formatos.

Para el análisis de vulnerabilidades y tráfico de red en aplicaciones que trabajen en sitios web, se recomienda utilizar herramientas que ayuden a identificar problemas de seguridad informática, a continuación, se hace un análisis de las herramientas más utilizadas para diagnosticar problemas de red, realizar auditorías de seguridad.

A continuación, se presenta un grupo de herramientas que también pueden ser una opción para detectar vulnerabilidades, se acota que en el presente proyecto no se hace uso de las siguientes herramientas:

Tabla 8

Otras herramientas de detección de vulnerabilidades.

Herramienta	Wireshark	Burpsuite	Ettercap
Característica			

Captura de paquetes	En tiempo real se realiza un análisis capturando el tráfico de la red donde se esté conectando.	Analiza el tráfico en la web.	Manipula el tráfico de la red conectada.
Protocolos	Permite la identificación y funcionamiento de varios protocolos de red.	Identifica protocolos HTTP y HTTPS	Incluye protocolos ARP y TCP
Análisis de tráfico	Cuenta con herramienta para examinar el tráfico de la red.	Realiza análisis y manipula solicitudes de respuesta.	Analiza paquetes de la red conectada.
Documentación	Herramienta con documentación completa.	Incluye documentación básica.	Incluye documentación básica.

Nota. En la tabla se muestra otras herramientas que se puede utilizar para la detección de vulnerabilidades.

En la Tabla 8 se describe un grupo las herramientas más utilizadas, la más recomendada Wireshark para diagnosticar problemas de red, realizar auditorías de seguridad o diagnóstico de problemas de red, se puede identificar vulnerabilidades en el tráfico de red en aplicaciones que trabajen en sitios web, se recomienda utilizar herramientas que ayuden a identificar problemas de seguridad informática, se hace un análisis de las herramientas más utilizadas para diagnosticar problemas de red, realizar auditorías de seguridad.

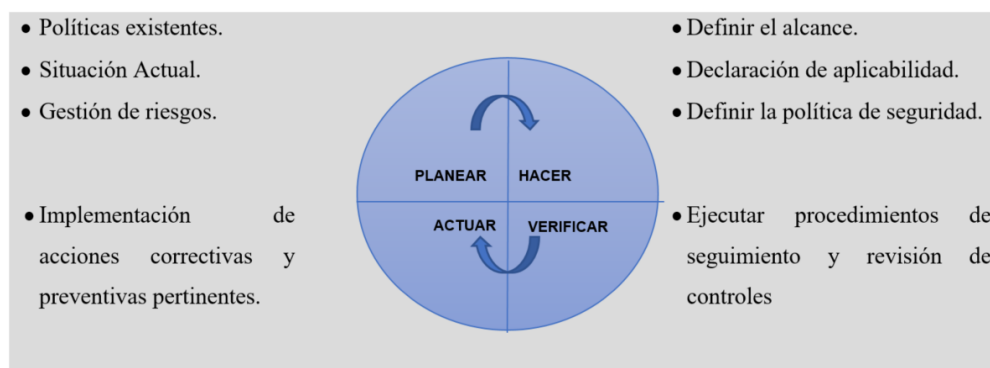
4.3 METODOLOGÍA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Para llevar a cabo un modelo de gestión de la seguridad de la información se adoptó la metodología DEMING también conocida como mejora continua (PDCA), muy usual en los sistemas para la gestión de la seguridad. La razón del porque se seleccionó dicha metodología es por la mejora continua, garantizan el cumplimiento de sus actividades.

A continuación, en la Figura 5 se puede describir cómo actúa el ciclo de manera ordenada y clara garantizando la seguridad de los datos.

Figura 5

Fases de desarrollo en base a la metodología Deming PDCA



Nota. La figura muestra el ciclo PDCA y su estructura general con relación a la norma ISO/IEC 27002.

PLANEAR

1. Políticas existentes en el Departamento de Administración de Redes

El departamento de Administración de Redes de la FISEI, al formar parte de la Universidad Técnica de Ambato se rige a las “Políticas Generales de Seguridad de la Información” de la institución antes mencionada, mismas que son puestas en conocimiento mediante el Oficio Nro. UTA-DITIC-2022-0005-O.

Estas políticas son generales las cuales palpando la realidad de la FISEI como facultad que genera recursos para adquirir infraestructura tecnológica y demás recursos necesarios se ve en la necesidad de llevar un estudio personalizado en cuanto a cómo se lleva la gestión de la información y al ser una facultad que tiene su propio Departamento para llevar a cabo la administración de la red de la institución.

Con la finalidad de mejorar el ámbito de la seguridad de la información y junto a los procesos que maneja la DITIC, mismos que hacen referencia a la reglamentación de normas ISO/IEC 27002, se lleva a cabo un análisis de cumplimiento y verificación de que está faltando mejorar en la institución y brindar un mejor servicio a la comunidad universitaria.

2. Situación actual de la Institución

Con la finalidad de conocer el estado actual que atraviesa la FISEI, se realizó un análisis detenido sobre los aspectos más relevantes para conocer el lugar donde se va a trabajar haciendo énfasis al departamento de Administración de Redes.

Evaluación de riesgos

Listado de direcciones IP de los activos informáticos críticos de la FISEI

En la Tabla 9, se puede apreciar a detalle los activos de información críticos junto con información relevante, que muestra la situación real de la institución donde se realiza la investigación y tomar las mejores decisiones para combatir los problemas de seguridad de la información.

Tabla 9

Listado de activos informáticos críticos de la FISEI

Nº	Dirección IP	Nombre	Sistema Operativo	Observaciones
1	172.XX.XX.13	Servidor de aplicaciones FISEI GenDocs v2.0.	Alma Linux Versión 8.4	El equipo almacena sistemas informáticos que se vayan desarrollando en la FISEI, así como servicios que contribuyan en la educación universitaria.
2	172.XX.XX.100	Cámaras de la FISEI.	Software Hikvision Versión DS-9664NI-I8	Este equipo está encargado de grabar las cámaras de aulas, pasillos, y laboratorios específicamente del Bloque 2 de la FISEI.
3	172.XX.XX.200	Cámaras de la FISEI.	Software Hikvision Versión DS-9664NI-I8	Este equipo está encargado de grabar las cámaras de aulas, pasillos, y laboratorios específicamente del Bloque 1 de la FISEI.
4	172.XX.XX.217	Administración de Redes.	Windows 10 Pro N	Equipo que aloja el sistema GenDocs y donde realizan cambios en el mismo sistema, se pone a prueba y a producción.

5	172.XX.XX.212	Coordinación de la Unidad de Vinculación FISEI.	Windows 10 Pro N	Equipo que almacena la coordinación, convenios, programas y proyectos de vinculación cumplidos en los últimos 5 años.
6	172.XX.XX.55	Unidad Académica de Titulación. Planificación y Evaluación Institucional.	Windows 10 Pro N	Almacena los procesos académicos de graduación del estudiantado de la FISEI. Almacena los programas de procesos técnicos y sistemáticos de planificación y evaluación institucional.
7	172.XX.XX.123	Equipo de almacenamiento de programas de la Unidad de Titulación de Posgrado de la FISEI.	Windows 10	Almacena la información de los últimos 5 años correspondiente a los programas de maestría cumplidos por la FISEI.
8	172.XX.XX.15	Unidad de Titulación de Posgrado de la FISEI.	Windows 10 Pro N	Equipo maneja y almacena los procesos correspondientes a la Unidad de Titulación de Posgrado de la FISEI.
9	172.XX.XX.203	Secretaría de Información – FISEI.	Windows 10	Equipo maneja y almacena los procesos correspondientes al ingreso de todos los requerimientos solicitados a la FISEI, así como la coordinación de registro de asistencia docente.
10	172.XX.XX.200	Secretaría de Decanato.	Windows 10 Pro N	Equipo encargado de almacenar los procesos desarrollados por el decanato.
11	172.XX.XX.206	Secretaría Sub Decanato	Windows 10 Pro N	Equipo encargado de almacenar los procesos desarrollados por el decanato.

Nota. Esta tabla muestra la identificación de los activos de información críticos de la FISEI.

Identificación y tasación de activos

Los activos informáticos son el principal componente que permite llevar a cabo los procesos que se realizan en la institución, los principales activos son: software, hardware y sistemas de información.

Estos recursos son uno de los más importantes en una organización dado a que por estos medios se manipula la información por lo que se debe dar el seguimiento correspondiente, ya identificados los activos existentes se procede a priorizar los de mayor importancia, basándose en los niveles de integridad, disponibilidad, confidencialidad de la información.

En cuanto al proceso de evaluación de los activos se establece un rango general entre 1 y 5, siendo 5 el de mayor importancia y van disminuyendo hasta el de menos importancia con el valor de 1 a continuación, en la Tabla 10 se puede apreciar la identificación y tasación de riesgos.

Tabla 10*Identificación y Tasación de riesgos*

Activos	Confidencialidad	Disponibilidad	Integridad	Total
Servidor de procesos a graduados.	5	4	4	4
Computadores del personal administrativo	3	4	3	3
Computadoras d estudiantes	2	4	2	2
Switch	3	4	3	3
Router	4	4	3	4
NVRs	4	4	4	4
Central Telefónica IP	2	4	4	3
Sistema desarrollado para graduaciones de la FISEI (GenDocs).	5	4	4	4
Sistema Seguimiento a graduados	3	3	4	3
Impresoras Multifuncional	3	4	3	3

Nota. En la tabla se muestra la Identificación y Tasación de riesgos con respecto a la confidencialidad, disponibilidad e integridad.

Una vez tasados los activos se define la probabilidad de ocurrencia con relación a las amenazas considerando el impacto que tendrá en caso de que ocurra, lo que da como resultado un riesgo a la confidencialidad disponibilidad e integridad de la información.

Como siguiente proceso se debe identificar los activos cuyos valores son mayores o iguales a 3, y poder calcular la probabilidad del riesgo, como se puede observar en la Tabla 11 corresponde a los activos con mayor importancia encontrados a cargo del departamento de Administración de Redes de la institución. Para obtener el valor del riesgo se debe multiplicar el valor total de la tasación del activo por el valor de la probabilidad de ocurrencia.

Tabla 11

Activos con mayor grado de importancia.

Activo	Amenazas	Vulnerabilidades	Valoración del activo	Probabilidad de amenaza	Riesgo Total
Servidor de Archivos	Alteración de información	Escasez de medidas de seguridad	4	3	12
	Robo de información	Falta de mantenimiento			
Computadores del personal administrativo	Phishing	Escasez de herramientas de monitoreo de correo	3	4	12
	Virus	Falta de mantenimiento			
	Malware	Uso inapropiado de internet			
	Spyware	Falta de control de acceso			
Switch	Recalentamiento	Problemas en el sistema eléctrico	3	4	12
	Daño o pérdida total	Falta de un UPS			
	Bajo rendimiento	Falta de mantenimiento			
	Blanqueamiento	Falta de control de accesos a las áreas restringidas.			
		Falta de seguridades.			
Router	Recalentamiento	Problemas en el sistema eléctrico	4	4	16
		Falta de un UPS			

	Daño o pérdida total				
	Bajo rendimiento	Falta de mantenimiento			
Router	Blanqueamiento	Falta de control de accesos a las áreas restringidas.	4	4	16
		Falta de seguridades.			
NVRs	Fuga de Información	Falta de control de acceso	4	4	16
	Daño en los dispositivos de almacenamiento	Falta de mantenimiento			
Central telefónica IP	Perdida de la conexión	Mala configuración de la central telefónica	3	2	6
Sistema GenDocs	Fuga de Información	Falta de control de acceso	4	2	8
	Robo de Información	Falta de políticas de seguridad			
	Robo de Información	Falta de políticas de seguridad			
Sistema Seguimiento a graduados	Fuga de Información	Falta de control de acceso	3	2	6
	Robo de Información	Falta de políticas de seguridad			
Impresor Multifuncional	Daño en los cartuchos	Falta de mantenimiento	3	4	12
	Cabezales dañados				

Impresor Multifunciona I	Falta de tinta	Falta de control de recursos	3	4	12
	Cartuchos incompatible				
	Atasco de papel	Inadecuado formato de papel			

Nota. En la tabla se muestra la valoración de los activos con mayor importancia en la FISEI.

Una vez realizado el análisis y evaluación de riesgos existentes, se pudo detectar de una manera más precisa cuales son los activos con los valores altos de criticidad correspondientes a la afección en el caso de que se materialicen estas amenazas dando origen a posibles ataques externos o internos dañando el buen funcionamiento de la institución.

4.4 Selección de Objetivos de control en base a la NORMA ISO/IEC 27002

En base a lo propuesto en el trabajo de investigación se hace uso de las buenas prácticas establecidas por la Norma ISO/IEC 27002, a continuación, haciendo uso de las condiciones de evaluación realizada en la Tabla 11, se añade una columna identificada como “Objetivo de Control”, con la finalidad de tener claro cuál es la amenaza que afecta a cada activo informático.

Hay que tener en cuenta que la selección correcta de los objetivos de control permitirá asegurar que cada activo de información sea valorado con el grado de riesgo correspondiente para ser cubierto y posteriormente auditable.

A continuación, se puede observar en la Tabla 12, como se añadió una columna “Objetivo de control”, la misma que contendrá los respectivos controles correspondientes a las amenazas detalladas por cada activo informático, esto en base a los controles pertenecientes a la norma ISO/IEC 27002.

Tabla 12

Relación que existe entre los objetivos de control de la Norma ISO/IEC 27002 y los activos informáticos críticos de la FISEI.

Activo	Amenazas	Vulnerabilidades	Valoración del activo	Probabilidad de amenaza	Riesgo Total
Servidor de Archivos	Alteración de información	Escasez de medidas de seguridad	4	3	12
	Robo de información	Falta de mantenimiento			
Computadores del personal administrativo	Phishing	Escasez de herramientas de monitoreo de correo	3	4	12
	Virus	Falta de mantenimiento			
	Malware	Uso inapropiado de internet			
	Spyware	Falta de control de acceso			
Switch	Recalentamiento	Problemas en el sistema eléctrico	3	4	12
	Daño o pérdida total	Falta de un UPS			
	Bajo rendimiento	Falta de mantenimiento			
Switch	Blanqueamiento	Falta de control de accesos a las áreas restringidas.			
		Falta de seguridades.			
Router	Recalentamiento	Problemas en el sistema eléctrico	4	4	16
	Bajo rendimiento	Falta de un UPS			
		Falta de mantenimiento			
	Blanqueamiento	Falta de control de accesos a las áreas restringidas.			
Falta de seguridades.					
NVRs	Fuga de Información	Falta de control de acceso	4	4	16
	Daño en los dispositivos de almacenamiento	Falta de mantenimiento			

Central telefónica IP	Perdida de la conexión	Mala configuración de la central telefónica	3	2	6
Sistema GenDocs	Fuga de Información	Falta de control de acceso	4	2	8
	Robo de Información	Falta de políticas de seguridad			
Sistema Seguimiento a graduados	Fuga de Información	Falta de control de acceso	3	2	6
	Robo de Información	Falta de políticas de seguridad			
Impresor Multifuncional	Daño en los cartuchos	Falta de mantenimiento	3	4	12
	Cabezales dañados				
	Falta de tinta	Falta de control de recursos			
	Cartuchos incompatible				
Atasco de papel	Inadecuado formato de papel				

Nota. En la tabla se muestra el resultado de la valoración del activo y su relación con la probabilidad de amenaza, obteniendo como resultado un riesgo total, con la finalidad de aplicar una medida de control en base a la norma ISO/IEC 27002

Historia de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial

A continuación, se describe la Historia de la FISEI, así como una imagen del sitio donde se realiza el proyecto de investigación Figura 6, con la finalidad de dar a conocer la institución.

“La Facultad de Ingeniería en Sistemas, Electrónica e Industrial (FISEI) de la Universidad Técnica de Ambato (UTA), se crea como Escuela de Informática y Computación, mediante resolución de H. Consejo Universitario No. 347-91-CU-P del 13 de octubre de 1991.

Los rápidos cambios y avances del mundo moderno, necesidades de automatización de las empresas públicas y privadas, que requerían profesionales en Informática a nivel de ingeniería, hicieron necesario realizar cambios en los planes y programas de estudio, para que, mediante resolución de H. Consejo Universitario No. 386-92-CU-P del 4 de agosto de 1992 pase a ser la Facultad de Ingeniería en Sistemas”. (FISEI, 2023).

Figura 6

Facultad de Ingeniería en Sistemas Electrónica e Industrial



Nota. Obtenido de la página oficial de la Facultad de Ingeniería en Sistemas Electrónica e Industrial

MISIÓN Y VISIÓN

MISIÓN

Formar profesionales líderes competentes, con visión humanista y pensamiento crítico, a través de la Docencia, la Investigación y la Vinculación, que apliquen, promuevan y difundan el conocimiento respondiendo a las necesidades del país (FISEI, 2023).

VISIÓN

La Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, por sus niveles de excelencia, se constituirá como un centro de formación superior con liderazgo y proyección nacional e internacional (FISEI, 2023).

En la Figura 7, se muestra el organigrama estructural correspondiente al departamento de Administración de Redes de la FISEI.

Figura 7

Estructura organizacional de Administración de Redes de la FISEI.



Nota. La figura muestra el organigrama estructural de la facultad. Tomado de la documentación interna compartida por la FISEI.

Principales funciones del personal del departamento de Administración de Redes FISEI

De la Tabla 13 a la Tabla 17 se muestra las diferentes funciones del personal perteneciente al área de Administración de Redes, en base a los objetivos y necesidades propias del departamento

Tabla 13

Descripción de funciones del Administrador de Redes

FUNCIONES ADMINISTRADOR/A DE REDES	Objetivo: Coordinar las actividades referentes a TI en la FISEI
Administrar el departamento de redes y sus dependencias.	
Administración de la red interna de comunicaciones de acuerdo a la configuración de la Institución.	
Coordinar el área de soporte técnico Administración de la infraestructura de redes y telecomunicaciones.	
Administración de equipos activos y pasivos de la red.	
Manejo del inventario de equipos de red y servidores.	

Controla el funcionamiento de los Laboratorios.
Establece las políticas de seguridad de las laboratorios
Administrar el sistema de antivirus y las herramientas asociadas a éste.
Supervisa mantenimiento a equipos informáticos.
Configuración de Servidores y Servicios de acuerdo a las necesidades de la institución.
Informes técnicos para la adquisición y recepción de equipos informáticos y redes de comunicación, de acuerdo a los requerimientos de la Facultad.
Proporcionar servicio de soporte técnico a estudiantes, al personal administrativo y docentes de la Facultad
Mantenimiento del Sistema de Vigilancia.
Administración de las cámaras de video vigilancia.
Asesoramiento técnico a Auxiliares de Laboratorio de la Facultad.
Elaboración de oficios.
Elaboración de Horarios
Capacitación Docentes, Administrativos y Estudiantes
Soporte técnico en el Sistema de Registro Docente
Actividades que requiera la facultad.
Mantenimiento del Sistema de Vigilancia.
Administración de las cámaras de video vigilancia.

Nota. La tabla muestra las funciones del Administrador de Redes, basado en la información proporcionada por dicho departamento.

Tabla 14

Funciones del Técnico de Laboratorio (Carrera de Sistemas)

FUNCIONES TÉCNICO DE LABORATORIO CARRERA DE SISTEMAS	Objetivo: Brindar soporte técnico garantizando el correcto funcionamiento del hardware y software de la FISEL.
Préstamo de equipos de la carrera de electrónica.	
Mantenimiento preventivo, correctivo y predictivo de equipos de la carrera de electrónica.	
Custodiar los materiales, equipos y programas asignados a los laboratorios.	
Asistencia técnica a los docentes, estudiantes y personal administrativo.	
Mantenimiento de las mesas de trabajo de los laboratorios de la carrera de electrónica.	
Instalar software especializado y/o actualizaciones autorizados.	
Control de equipos prestados a los Docentes para sus clases y recuperación en los mismos.	
Verificación del correcto funcionamiento de los equipos.	

Reportar y atender las fallas que puedan presentar los equipos.
Controlar el inventario de los recursos del laboratorio.
Velar por el cumplimiento de las normas y procedimientos establecidos.
Mantener en orden equipos y sitios de trabajo, reportando cualquier anomalía.
Elaborar registros de mantenimiento de los equipos de la carrera de electrónica.
Colaboración en todas las actividades y eventos de la facultad.
Colaboración con los señores Docentes.
Otras actividades requeridas por Decanato y Administración de Redes FISEI.
<i>Nota.</i> La tabla muestra las funciones del Técnico de Laboratorio de la carrera de Sistemas, basado en la información proporcionada por dicho departamento.

Tabla 15

Funciones del Técnico de Laboratorio (Carrera de Electrónica)

FUNCIONES TÉCNICO DE LABORATORIO CARRERA DE ELECTRÓNICA	Objetivo: Garantizar el buen funcionamiento de la infraestructura de servidores y redes.
Préstamo de equipos.	
Mantenimiento preventivo, correctivo y predictivo de equipos.	
Custodiar los materiales, equipos y programas asignados a los laboratorios.	
Instalar software especializado y/o actualizaciones autorizados.	
Limpieza de Hardware y Software de equipos de computación.	
Asistencia técnica a los docentes, estudiantes y personal administrativo.	
Respaldar y organizar datos almacenados en los equipos.	
Revisión periódica de infecciones de virus, actualización de antivirus en los laboratorios.	
Asistir en la administración de la red local de la Facultad.	
Control de equipos prestados a los Docentes para sus clases y recuperación en los mismos.	

Nota. La tabla muestra las funciones del Técnico de Laboratorio de la carrera de Electrónica, basado en la información proporcionada por dicho departamento.

Tabla 16

Funciones del Técnico de Laboratorio (Carrera de Electrónica)

FUNCIONES TÉCNICO DE LABORATORIO CARRERA DE ELECTRÓNICA	Objetivo: Garantizar el buen funcionamiento de la infraestructura de servidores y redes.
Reportar y atender las fallas que puedan presentar los equipos.	

Controlar el inventario de los recursos del laboratorio.
Configuración y habilitación de puntos de Red.
Velar por el cumplimiento de las normas y procedimientos establecidos.
Mantener en orden equipos y sitios de trabajo, reportando cualquier anomalía.
Elaborar registros de mantenimiento de los equipos.
Colaboración en todas las actividades y eventos de la facultad.
Colaboración con los señores Docentes.
Administración de la Página Web de la FISEI.
Asistencia técnica a la comunidad universitaria.
Apoyo a la Comisión de Graduados de la FISEI.
Mantenimiento Preventivo y Correctivo de los Equipos de los Laboratorios del FISEI-UTA.
Mantenimiento y Soporte de Equipos Informáticos de la Colectividad.
Mantenimiento de equipos CISCO del FISEI-UTA.
Otras actividades requeridas por Decanato y Administración de Redes FISEI.

Nota. La tabla muestra las funciones del Técnico de Laboratorio de la carrera de Electrónica, basado en la información proporcionada por dicho departamento.

Tabla 17

Funciones del Técnico de Laboratorio (Carrera de Industrial)

FUNCIONES TÉCNICO DE LABORATORIO CARRERA DE INDUSTRIAL	Objetivo: Ayudar en el soporte a estudiantes y docentes en laboratorios especializados, actividades técnicas y de ofimática.
Préstamo de equipos de la carrera de Industrial.	
Verificación del funcionamiento de los módulos del Laboratorio de PLC's.	
Comprobación de equipos en los laboratorios informáticos de la carrera de Industrial	
Custodiar los materiales, equipos y programas asignados a los laboratorios.	
Asistencia técnica a los docentes, estudiantes y personal administrativo.	
Sustitución de elementos dañados de laboratorios informáticos de la carrera de Industrial	
Control de equipos prestados a los Docentes para sus clases y recuperación en los mismos.	
Revisión del funcionamiento de equipos hidráulicos y neumáticos del Laboratorio de Hidráulica.	

Comprobación del correcto funcionamiento de fresadores CNC del laboratorio de CNC
Controlar el inventario de los recursos del laboratorio.
Velar por el cumplimiento de las normas y procedimientos establecidos.
Mantener en orden equipos y sitios de trabajo, reportando cualquier anomalía.
Elaborar registros de mantenimiento de los equipos de la carrera de electrónica.
Colaboración en todas las actividades y eventos de la facultad.
Asistencia Técnica a Instructores y participantes Cursos CTT-FISEI-UTA
Otras actividades requeridas por Decanato y Administración de Redes FISEI.

Nota. La tabla muestra las funciones del Técnico de Laboratorio de la carrera de Industrial, basado en la información proporcionada por dicho departamento.

Requerimientos de Software instalado en los laboratorios, personal administrativo y docentes

En la Tabla 18 y Tabla 19 se puede visualizar el Software instalado en los equipos informáticos de la FISEI junto con la versión, la cual los docentes trabajan con los estudiantes y el personal administrativo de la institución.

Tabla 18

Requerimientos de software instalado en los Laboratorio de la FISEI Periodo 2023-2024

REQUERIMIENTOS DE SOFTWARE INSTALADO EN EL LABORATORIO 1		
PERIODO 2023-2024		
DOCENTE	SOFTWARE	VERSIÓN
LABORATORIO 1		
CLAY ALDÁS	GIT	ÚLTIMA VERSIÓN
	ANDROID STUDIO	ÚLTIMA VERSIÓN
	FLUTTER	ÚLTIMA VERSIÓN
	FIGMA	ÚLTIMA VERSIÓN

	ADOBE XD	ÚLTIMA VERSIÓN
HERNÁN NARANJO	VISUAL STUDIO COMMUNITY	2022
	MANAGEMENTR STUDIO	18.12.1
	SQL SERVER EXPRESS	ÚLTIMA VERSIÓN
	ANACONDA	ÚLTIMA VERSIÓN
	MONGO DB	ÚLTIMA VERSIÓN
LEONARDO TORRES	STARTUML	ÚLTIMA VERSIÓN
FÉLIX FERNANDEZ	NETBEANS	8.2 RC
LABORATORIO 2		
CARLOS NUÑEZ	NETBEANS	ÚLTIMA VERSIÓN
	XAMMP	ÚLTIMA VERSIÓN
	POSTMAN	ÚLTIMA VERSIÓN
LABORATORIO 3		
MARCO GUACHIMBOZA	R STUDIO	ÚLTIMA VERSIÓN
	NETBEANS	12.5 O +
	JDK JAVA	17.0.1
JULIO BALAREZO	ORACLE VM VIRTUALBOX	7.0.12
PABLO MORALES	SQL SERVER	ÚLTIMA VERSIÓN
	V STUDIO INTEGRATION SERV	ÚLTIMA VERSIÓN
LABORATORIO 4		
SANTIAGO JARA	XAMPP	ÚLTIMA VERSIÓN
	NETBEANS	ÚLTIMA VERSIÓN
	DOXYGEN	ÚLTIMA VERSIÓN
	JMETER	ÚLTIMA VERSIÓN
FERNANDO IBARRA	VISUAL STUDIO CODE	1.6
	MYSQL	7
	MYSQLWORKBENCH	6
PABLO MORALES	JUNIT FRAMEWORK PARA	ÚLTIMA VERSIÓN

	NETBEANS	
LABORATORIO 5		
VÍCTOR GUACHIMBOZA	PROJECT	ÚLTIMA VERSIÓN
JULIO BALAREZO	VIRTUALBOX	7.0.6
PABLO MORALES	XAMMP	ÚLTIMA VERSIÓN
	MYSQL WORKBENCH	ÚLTIMA VERSIÓN
	ORACLE	ÚLTIMA VERSIÓN
LABORATORIO 6		
HERNÁN NARANJO	VISUAL STUDIO COMMUNITY	2022
	VISUAL STUDIO CODE	ÚLTIMA VERSIÓN
FRANLIN MAYORGA	JABREF	5.7
	MENDELEY ESCRITORIO	ÚLTIMA VERSIÓN
	OFFICE	365
LABORATORIO 7		
RUBÉN NOGALES	SQL SERVER	ÚLTIMA VERSIÓN
	MARIA DB	ÚLTIMA VERSIÓN
	.NET INTEGRATIONS SERVICES	ÚLTIMA VERSIÓN
	MATLAB	ÚLTIMA VERSIÓN
	PHYTON -ANACONDA	ÚLTIMA VERSIÓN
	PROLOG	ÚLTIMA VERSIÓN
	LATEX	ÚLTIMA VERSIÓN
	MENDELEY	ÚLTIMA VERSIÓN
	LYX	ÚLTIMA VERSIÓN
	R-STUDIO	ÚLTIMA VERSIÓN
LEONARDO TORRES	SQL SERVER DEVELOPER MANAGEMENT STUDIO	2022
		19
LABORATORIO 8		
	WIRESHARK	4.0.8

DENNIS CHICAIZA	PACKET TRACER	8.2.1
	NODEJS	18.17.1
	ANDROID STUDIO	GIRAFFE

FÉLIX FERNANDEZ	NETBEANS	8.2 RC

HERNÁN NARANJO	VISUAL STUDIO	2022
	MANAGEMENTR STUDIO	18.12.1
	VISUAL CODE	ÚLTIMA VERSIÓN
	SQL SERVER EXPRESS	ÚLTIMA VERSIÓN
	ANACONDA	ÚLTIMA VERSIÓN

FRANKLN MAYORGA	VIRTUAL BOX	
	MAQUINA VIRTUAL CENTOS 7	7

PABLO MORALES	NETBEANS	15
----------------------	----------	----

LABORATORIO CTT

EDISON ÁLVAREZ	SQL SERVER 2022	ENTERPRISE
	VISUAL STUDIO 2022	ENTERPRISE
	POWER BI DESKTOP	ÚLTIMA VERSIÓN
	PHYTON	3.11.5 O +

FRANKLIN MAYORGA	JABREF	5.7
	MENDELEY ESCRITORIO	ÚLTIMA VERSIÓN
	OFFICE	365

LEONARDO TORRES	PSEINT	ÚLTIMA VERSIÓN
	NETBEANS	ÚLTIMA VERSIÓN
	JAVA	8

LABORATORIO REDES 1

DAVID GUEVARA	ORACLE VM VIRTUALBOX	7.0.12
----------------------	----------------------	--------

FRANKLIN MAYORGA	JABREF	5.7
	MENDELEY ESCRITORIO	ÚLTIMA VERSIÓN
	OFFICE	365

DANIEL JERÉZ	PSEINT	ÚLTIMA VERSIÓN
	NETBEANS	ÚLTIMA VERSIÓN
	JAVA	8
PILAR URRUTIA	CISCO PACKET TRACER	ÚLTIMA VERSIÓN

Nota. En la tabla se muestra como una descripción del Software instalado en los Laboratorios de la FISEI.

Tabla 19

Requerimientos de software instalado en el personal Administrativo y Docentes de la FISEI Periodo 2023-2024

REQUERIMIENTOS DE SOFTWARE INSTALADO EN EL PERSONAL ADMINISTRATIVO Y DOCENTE PERIODO 2023-2024		
PERSONAL	SOFTWARE	VERSIÓN
PERSONAL DOCENTE	ORACLE VM VIRTUALBOX	7.0.12
	ACROBAT READER	ÚLTIMA VERSIÓN
	JABREF	5.7
	MENDELEY ESCRITORIO	ÚLTIMA VERSIÓN
	OFFICE	365
	NOTEPAD ++	8.5.8
	PSEINT	ÚLTIMA VERSIÓN
	NETBEANS	ÚLTIMA VERSIÓN
	JAVA	8
	VLC	ÚLTIMA VERSIÓN
	CISCO PACKET TRACER	ÚLTIMA VERSIÓN
	7 ZIP	23.01
	GIT BASH	2.42.1
PERSONAL ADMINISTRATIVO	VLC	ÚLTIMA VERSIÓN
	VISUAL CODE	1.84
	OFFICE	2013
	7 ZIP	23.01
	NAVEGADORES CHROME	ÚLTIMA VERSIÓN
	NAVEGADORES FIREFOX	ÚLTIMA VERSIÓN
	ACROBAT READER	ÚLTIMA VERSIÓN
	NOTEPAD ++	8.5.8
OFFICE	2013	

Nota: En la tabla se muestra como una descripción del Software instalado para el personal docente y administrativo de la FISEI.

Principales características de la infraestructura de la red de la FISEI

La infraestructura de red de la FISEI surge como necesidad crítica en la era digital actual, esencial para un eficiente funcionamiento institucional. Para llegar a cumplir el objetivo de analizar los riesgos de vulnerabilidad de la información del departamento de Administración de Redes de la FISEI, se desarrolló un mapeo de red utilizando la herramienta Draw.io cuyo software es libre, permitiendo realizar el diagrama de red de manera clara e identificando que tipo de equipos son clave para desarrollar un modelo de gestión de la seguridad de la información, ya que las estructura de la institución está

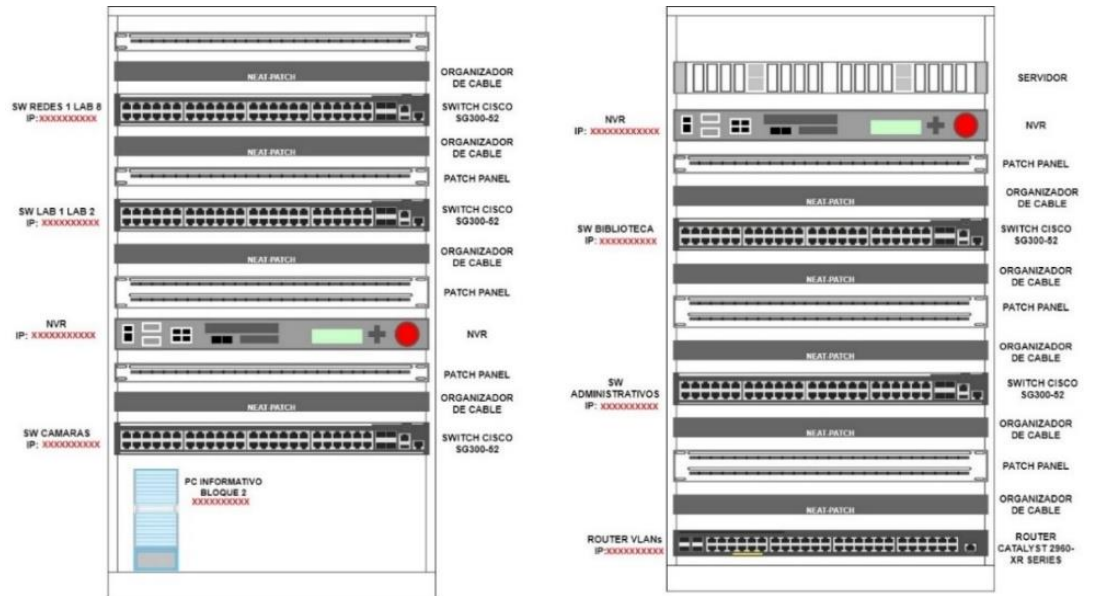
constituida por laboratorios de computación distribuidos por VLANs como se puede apreciar en Anexos II, por motivos de confidencialidad no se muestra el detalle de la VLAN en cada ambiente de la FISEI.

Dado a su exigencia por dar este gran paso tecnológico su implementación fue desordenada, poco flexible para un crecimiento futuro. La red de la institución se encuentra diseñada con una topología en forma de árbol misma que se encuentra estructurada de la siguiente manera:

1. La infraestructura de FISEI cuenta con dos bloques principales y una edificación utilizada como talleres tecnológicos, todos estos ubicados en el campus de Huachi Chico.
2. El Bloque 1, consta de un enlace mediante GPON y un Router Cisco Catalyst 2960XR administrado por la DITIC de la UTA, mismo de es de gran importancia ya que tiene configurado la segmentación de LAN virtual (VLAN) para las distintas dependencia como es personal administrativo, sala de docentes, salas de investigación, biblioteca, cámaras IP, y para los grupos de laboratorios, cuenta con una traducción de direcciones de red (NAT), mientras que el direccionamiento que utiliza esta realizado con IPv4.
3. La característica de este tipo de switches es que los puestos son POE donde se realiza la conexión a los AP's que permiten que los usuarios inalámbricos se conecten a la red y accedan a Internet inalámbrico en puntos estratégicos mismos permiten conectar a usuarios mediante DHCP.
4. A continuación, desde la Figura 8 hasta la Figura 11 se muestra cómo se encuentran estructurados respectivamente los principales RACKS de la FISEI. De la misma manera se puede evidenciar el Anexo II el mapa de red de los Bloque 1 y Bloque 2, en el cual se visualiza de mejor manera como se encuentra estructurada la red, así como la ubicación y distribución de los APs. Cabe recalcar que el mapa de red de la FISEI mostrado en Anexos II es realizado por autoría del investigador para fines investigativos del presente proyecto, y se deja material actualizado para el departamento de Administración e Redes como aporte de la presente investigación.

Figura 8

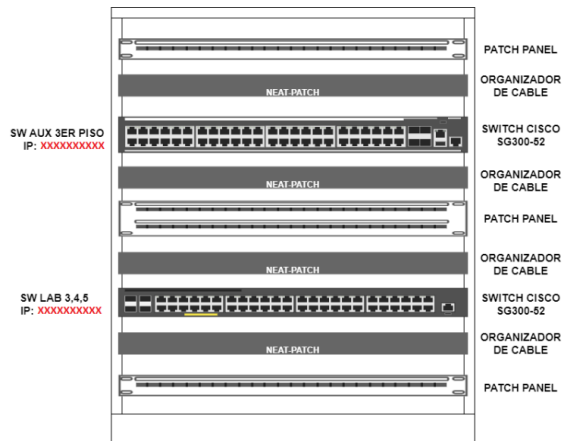
Estructura del Rack principal Bloque I



Nota. En la figura se muestra cómo se encuentran estructurados los principales RACKS de la FISEI (Bloque 1 segundo piso).

Figura 9

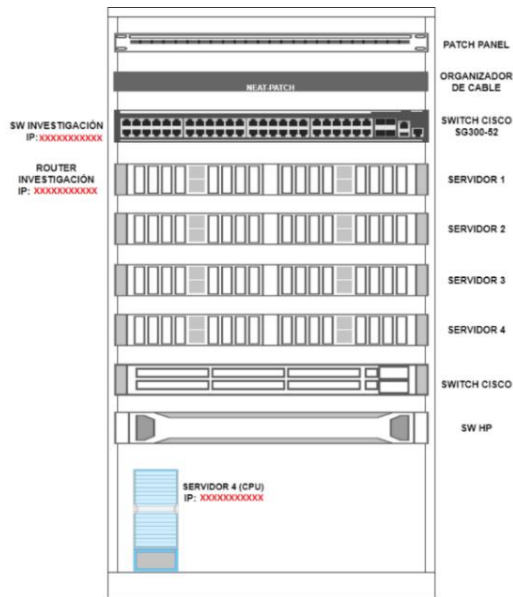
Estructura del Rack Bloque I (Tercer piso)



Nota. En la figura se muestra cómo se encuentra estructurado el RACK de la FISEI (Bloque 1 tercer piso).

Figura 10

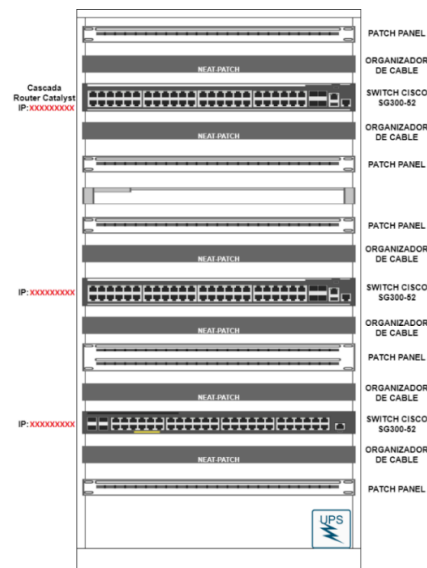
Estructura del Rack Bloque I (Sala de Investigación)



Nota. En la figura se muestra cómo se encuentra estructurado el RACK de la FISEI (Bloque 1 planta baja).

Figura 11

Estructura del Rack Bloque II



Nota. En la figura se muestra cómo se encuentra estructurado el RACK de la FISEI (Bloque 2 primer piso).

CAPÍTULO V

CONCLUSIONES, RECOMENDACIONES, BIBLIOGRAFÍA, ANEXOS.

5.1. Conclusiones

- En la FISEI, las directrices relacionadas con la gestión de la seguridad de la información no se implementan ni se documenta de manera eficaz.
- Se observa que, en parte, carecen de políticas, controles, normativas o sistemas de gestión de seguridad de la información. Como resultado, la disponibilidad, integridad y confidencialidad de la información en todas sus formas están expuestas a riesgos y amenazas.
- Se llevó cabo el análisis y evaluación del impacto en los activos críticos de información, ante los riesgos que se pueden identificar considerando los posibles escenarios y los procesos que se llevan a cabo en la institución.

5.2. Recomendaciones

- Se recomienda que en la FISEI se planteen estrategias de solución para evitar la materialización de las amenazas expuestas ante los activos informáticos críticos siendo los más urgentes.
- La FISEI al ser una facultad que forma estudiantes con habilidades y destrezas en temas informáticos, mediante la gestión interna se puede autorizar la elaboración de proyectos de titulación, que cubran las falencias identificadas en temas de seguridad informática aportando con nuevas políticas que sean aprobadas por la máxima autoridad de la facultad.
- Realizar una adecuación del entorno físico para los equipos informáticas críticos que procesan y albergan información relevante para la FISEI, con el objetivo de salvaguardar la integridad física de los mismos.

5.3. Bibliografía

- ISO/IEC 27002, S. e. (2020). *ISO/IEC 27002*. Obtenido de Tecnología de la información - Técnicas de seguridad - Código de prácticas para controles de seguridad de la información: <https://www.iso.org/standard/54533.html>
- 27000.ES, I. (28 de Julio de 2015). *Seguridad de la Información*. Obtenido de ISOTools: <https://www.pmg-ssi.com/2015/07/que-es-sgsi/>
- Academia, S. (Junio de 2021). *Universidad Tecnológica Empresarial de Guayaquil, Ecuador*. Obtenido de <https://doi.org/10.54753/suracademia.v8i15.927>
- AENOR. (08 de 10 de 2023). *AENOR*. Obtenido de <https://www.aenorecuador.com/certificacion/tecnologias-de-la-informacion/continuidad-negocio>
- Alexandra, E. (24 de Septiembre de 2018). *UNIVERSIDAD TÉCNICA DEL NORTE*. Obtenido de <http://repositorio.utn.edu.ec/handle/123456789/8572>
- Alonso, C. (30 de Marzo de 2023). *GlobalSuite Solutions*. Obtenido de <https://www.globalsuitesolutions.com/es/la-familia-de-normas-iso-27000/>
- Aranda, J. (22 de Noviembre de 2022). *UNIVERSIDAD TÉCNICA DE AMBATO*. Obtenido de UTA: https://repositorio.uta.edu.ec/bitstream/123456789/37007/1/Tesis_Pablo_Aranda.pdf
- Ariel Giannone, H. A. (12 de Octubre de 2018). *SEDIC Universidad Nacional de La Plata*. Obtenido de Congreso Argentino de Ciencias de la Computación: <http://sedici.unlp.edu.ar/handle/10915/73243>
- ASHRAE. (08 de 10 de 2023). *ANSI*. Obtenido de http://www.ditar.cl/archivos/Normas_ASHRAE/T0120ASHRAE-62.1-2007-sp-Ventil-p-CAAI.pdf
- B. Nour, S. M. (Abril de 2021). *IEEE*. Obtenido de 10.1109/MWC.001.2000245
- BICSI, A. (10 de 2023). *STANDARS BICSI*. Obtenido de <https://www.bicsi.org/standards/available-standards-store/single-purchase/ansi-bicsi-002-2019-data-center-design>
- Briceño, E. V. (marzo de 2021). *3 Ciencias*. Obtenido de Editorial Área de Innovación y Desarrollo,S.L.: <https://doi.org/10.17993/tics.2021.4>
- Camacho, V. (10 de Diciembre de 2021). *Escuela Politécnica Nacional*. Obtenido de EPN: <http://bibdigital.epn.edu.ec/handle/15000/21975>
- Castro, M. I. (Octubre de 2018). *Editorial Área de Innovación y Desarrollo,S.L*. Obtenido de <http://dx.doi.org/10.17993/IngyTec.2018.46>
- Cedeño, M. E. (15 de Noviembre de 2022). *Repositorio UTA*. Obtenido de UTA: <https://repositorio.uta.edu.ec/jspui/handle/123456789/37008>
- Charter, R. (2023). *BSI*. Obtenido de British Standards Institution: <https://www.bsigroup.com/es-ES/ISOIEC-20000-Gestion-de-Servicios/>
- Chávez, W. A. (2021). *Universidad Nacional de Trujillo., Perú*. Obtenido de Redalyc: <https://www.redalyc.org/journal/6738/673870839003/html/>
- Chomali, A. S. (2020). *Agenda Digital Regional eLAC*. Obtenido de CEPAL: https://repositorio.cepal.org/bitstream/handle/11362/45360/4/OportDigitalizaCovid-19_es.pdf

- Christian, G. (2021). *Universidad Técnica de Ambato*. Obtenido de <https://repositorio.uta.edu.ec/bitstream/123456789/36859/1/Granda%20Ar%c3%a9valo%20Christian%20Fernando.pdf>
- CISCO. (2023). *CISCO*. Obtenido de <https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html>
- EGSI. (5 de Agosto de 2022). *MINTEL*. Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/2022/10/anexo_acuerdo-No.-mintel-mintel-2022-0026.pdf
- Espinoza, G. C. (2020). *Investigación, Ciencia y Tecnología en Informática*. Obtenido de *Ethical Hacking: Conciencia de Seguridad*: https://ojs.umsa.bo/ojs/index.php/inf_fcpn_pgi/article/view/104/90
- Esteban, G. G. (07 de Septiembre de 2020). *EPN*. Obtenido de Repositorio Digital Institucional de la Escuela Politécnica Nacional: <http://bibdigital.epn.edu.ec/handle/15000/21377>
- F. Sechi, B. G.-A. (2022). *IEEE/ACM 3rd International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS)*. Obtenido de <https://doi.org/10.1145/3524489.3527304>
- Filho, F. C. (2023). *REDCEDIA*. Obtenido de <https://cedia.edu.ec/docs/efc/GTI7.pdf>
- FISEI. (2023). *FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL*. Obtenido de <https://fisei.uta.edu.ec/v4.0/index.php/facultad/historia-facultad>
- G. Muhamad Nur, R. L. (11 de Noviembre de 2022). *IEEE*. Obtenido de IEEE Xplore: <https://ieeexplore.ieee.org/document/9935943>
- Gashi, H. A. (22 de Octubre de 2021). *Springer Nature Switzerland AG*. Obtenido de <https://doi.org/10.1007/s10664-021-10046-w>
- Gracia, G. M. (20 de Enero de 2021). *Retos Revista de Ciencias de la Administración y Economía*. Obtenido de <https://doi.org/10.17163/ret.n21.2021.04>
- Hernández, A. F. (Agosto de 2020). *Universidad Internacional SEK*. Obtenido de SEK: <https://repositorio.uisek.edu.ec/bitstream/123456789/4010/1/Alfonso%20Fabi%c3%a1n%20Portilla%20Hern%c3%a1ndez.pdf>
- Humberto, A. M. (4 de Abril de 2019). *UNIVERSIDAD TÉCNICA DEL NORTE*. Obtenido de <http://repositorio.utn.edu.ec/handle/123456789/9028>
- ISO. (2022). *Organismos Nacionales de Normalización*. Obtenido de <https://www.iso.org/standards.html>
- ISO27000ES. (Octubre de 2013). *Iso27000.es*. Obtenido de <https://www.iso27000.es/iso27000.html>
- ITU. (2020). *Unión Internacional de Telecomunicaciones*. Obtenido de https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-S.pdf
- Julio, P. (Septiembre de 2019). *UNIVERSIDAD INTERNACIONAL SEK*. Obtenido de <http://repositorio.uisek.edu.ec/handle/123456789/3601>
- Lema Vinlasaca, R. C. (2018). *ESPE*. Obtenido de Repositorio ESPE: <http://repositorio.espe.edu.ec/handle/21000/14397>

- León, M. (Junio de 2021). *Universidad Tecnológica Empresarial de Guayaquil, Ecuador*. Obtenido de <https://doi.org/10.54753/suracademia.v8i15.927>
- Marco, G. (Julio de 2022). *Institucional de la Escuela Politécnica Nacional*. Obtenido de EPN: <http://bibdigital.epn.edu.ec/handle/15000/22812>
- Mendoza, P. (7 de Abril de 2020). *Escuela Politécnica Nacional*. Obtenido de <http://bibdigital.epn.edu.ec/handle/15000/20959>
- Miller, S. S. (s.f.). Defiéndose de los nuevos HACKERS. En *Seguridad en WiFi* (pág. 20). MCGRAW-HILL.
- Mintel. (Agosto de 2022). *Ministerio de Telecomunicaciones y Sociedad de la Información*. Obtenido de ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DEL ECUADOR: <https://asobanca.org.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-DEL-ECUADOR-2022481.pdf>
- Moya, C. (marzo de 2023). *PUCESA*. Obtenido de <https://repositorio.pucesa.edu.ec/bitstream/123456789/4088/1/79247.pdf>
- Paolo Frasca1, 2. B. (16 de septiembre de 2019). *Wiley Online Library*. Obtenido de <https://doi.org/10.1002/rnc.4794>
- Perkins, L. A. (08 de 10 de 2023). *Telecommunications Industry Association (TIA)*. Obtenido de TIA ONLINE: <https://tiaonline.org/products-and-services/tia942certification/>
- RACINES, F. (2023). *IAI ECUADOR*. Obtenido de https://iaiecuador.org/documentos/Programa_Tecnico_Certificado_Gestion_Riesgos_COSOERM_13Octubre.pdf
- Rincon, L. (2021). *Dialnet*. Obtenido de Universidad Rafael Belloso Chacín: <https://dialnet.unirioja.es/descarga/articulo/8577955.pdf>
- Salman, I. B. (29 de Agosto de 2022). *Cybersecurity Maturity Assessment Design Using NISTCSF, CIS CONTROLS v8 and ISO/IEC 27002*. Obtenido de 2022 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom): <https://ieeexplore.ieee.org/document/9865640>
- Suastegui Jaramillo, L. E. (07 de marzo de 2022). *Universidad Catolica de Santiago de Guayaquil*. Obtenido de <http://repositorio.ucsg.edu.ec/handle/3317/18016>
- Sulistyowati, D. (2020). *JOIV*. Obtenido de <http://dx.doi.org/10.30630/joiv.4.4.482>
- Técnicas, U. I. (2015). *UNIT*. Obtenido de <http://www.unit.org.uy/normalizacion/sistema/27000/>
- Unido, O. n. (08 de 10 de 2023). *BSI Group*. Obtenido de La Institución Británica de Normalización 2023: <https://standardsdevelopment.bsigroup.com/projects/9023-09086#/section>
- Villamizar, C. (25 de 09 de 2023). *Global Suite Solutions*. Obtenido de <https://www.globalsuitesolutions.com/es/que-es-cobit/>
- Wilson, C. (2019). *UNIVERSIDAD TÉCNICA DE AMBATO*. Obtenido de https://repositorio.uta.edu.ec/bitstream/123456789/29844/1/Tesis_t1585msi.PDF
- Zambrano, L. (2019). *UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD*. Obtenido de UNAD: <https://repository.unad.edu.co/bitstream/handle/10596/35641/pcborrero.pdf?sequence=3&isAllowed=y>

5.4. Anexos

Anexo I

ENTREVISTA AL ADMINISTRADOR DE REDES DEL ÁREA DE ADMINISTRACIÓN DE REDES DE LA UNIVERSIDAD TÉCNICA DE AMBATO (UTA), FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL (FISEI)

Nombre del encuestador: Ing. Saltos Ponce Cristian Javier **Ciudad:** Ambato

Lugar donde se aplica: Ambato/ Administración de Redes de la UTA FISEI

Fecha: 28/Mayo/2023

Estimado entrevistado: El motivo de la siguiente entrevista es conocer sobre los riesgos informáticos en el área de Administración de Redes de la UTA FISEI.

Nombre de entrevistado: Ing. Frutos Ortega Cristina Alexandra Mg.

Cargo que desempeña: Analista de TICs

Tiempo en la función: 12 AÑOS

Políticas de seguridad de la información

- ❖ ¿El departamento de Administración de Redes cuenta con políticas de seguridad de la información?
SI () NO ()
- ❖ ¿El personal técnico y administrativo de la UTA FISEI tiene conocimiento de las políticas de seguridad de la información?
SI () NO ()
- ❖ ¿Se ha implementado los controles de cumplimiento acerca de las políticas de seguridad de la información?
SI () NO ()
- ❖ ¿Se cuenta con políticas de seguridad que se encarguen de supervisar la manera en la que se manipula la información?
SI () NO ()
- ❖ ¿Los incidentes de seguridad de los sistemas de información son reportados brevemente por el personal?
SI () NO ()

Aspectos organizativos para la seguridad

- ❖ ¿Se cuenta con un área para uso exclusivo del desempeño de la seguridad de la información?
SI () NO ()
- ❖ ¿En el caso de migrar al teletrabajo, se cuenta con herramientas actualizadas y plataformas educativas para continuar con normalidad?
SI () NO ()

Con relación a la gestión de activos informáticos

- ❖ ¿Se cuenta con un inventario de activos de información actualizado?
SI () NO ()
- ❖ ¿El inventario esta automatizado?
SI () NO ()
- ❖ ¿El inventario de los activos informáticos es actualizado de manera periódica?
SI () NO ()
- ❖ ¿Los activos informáticos se encuentran correctamente etiquetados?
SI () NO ()

Con relación al control de acceso

- ❖ ¿En cuanto a las aplicaciones de la Universidad Técnica de Ambato y en la relación a las usadas en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, cuentan con políticas de control de acceso?
SI () NO ()
- ❖ ¿Se cuenta con un control de acceso a las redes y servicios asociados?
SI () NO ()
- ❖ ¿Se cuenta con procedimientos seguros para el inicio de sesión con relación al personal docente y área administrativa?
SI () NO ()
- ❖ ¿Se cuenta con procedimientos seguros para el inicio de sesión con relación al personal docente y área administrativa?
SI () NO ()
- ❖ ¿Para el acceso remoto se tiene establecidos mecanismos de autenticación de usuarios para el acceso a la red interna de la institución?
SI () NO ()

Con relación al cifrado

- ❖ ¿Para el uso y almacenamiento de la información por parte del personal de la institución cuenta con políticas de controles criptográficos?
SI () NO ()
- ❖ ¿Se gestiona las claves de manera segura de cada uno de las áreas y departamentos de la institución?

SI ()

NO ()

Con relación a la seguridad física y ambiental

- ❖ ¿Todas las áreas se encuentran correctamente identificadas?
SI () NO ()
- ❖ ¿Para acceder a las áreas seguras se cuenta con los respectivos controles y restricciones de ingreso del personal no autorizado?
SI () NO ()
- ❖ ¿En caso de alguna falla en los equipos informáticos se está preparados para su pronta corrección?
SI () NO ()
- ❖ ¿Se realiza mantenimiento periódico al hardware y software a los equipos informáticos de la institución?
SI () NO ()

Con relación a la seguridad en la operativa

- ❖ ¿Se realiza periódicamente copias de seguridad de la información (backups)?
SI () NO ()
- ❖ ¿Se lleva un control correspondiente a la gestión de las vulnerabilidades técnicas?
SI () NO ()
- ❖ ¿Se cuenta con restricciones en la instalación de software?
SI () NO ()
- ❖ ¿Se realiza controles de auditoría de los sistemas de información?
SI () NO ()

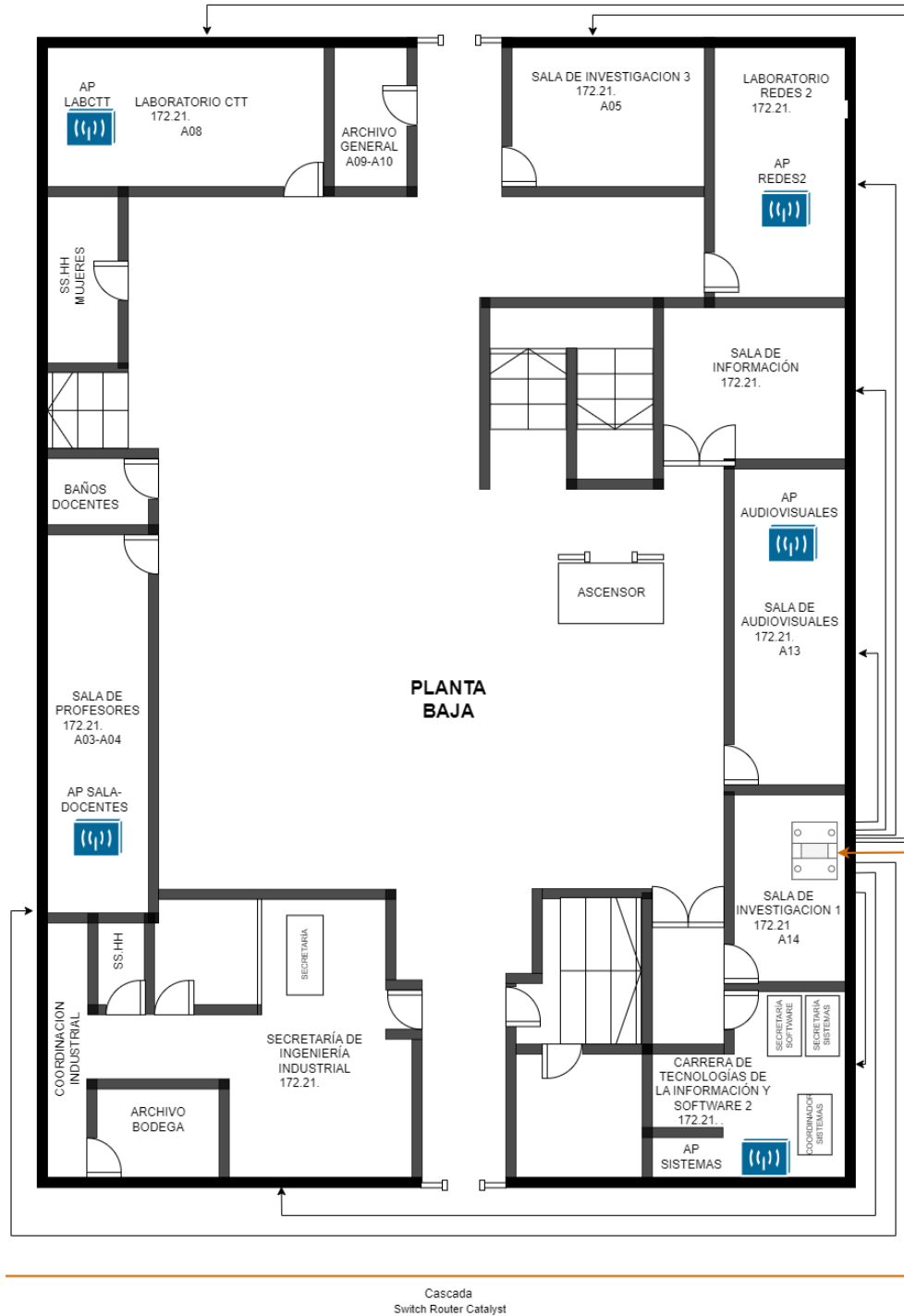
FIRMA

Ing. Cristina Frutos Mg.

Analista de TICs

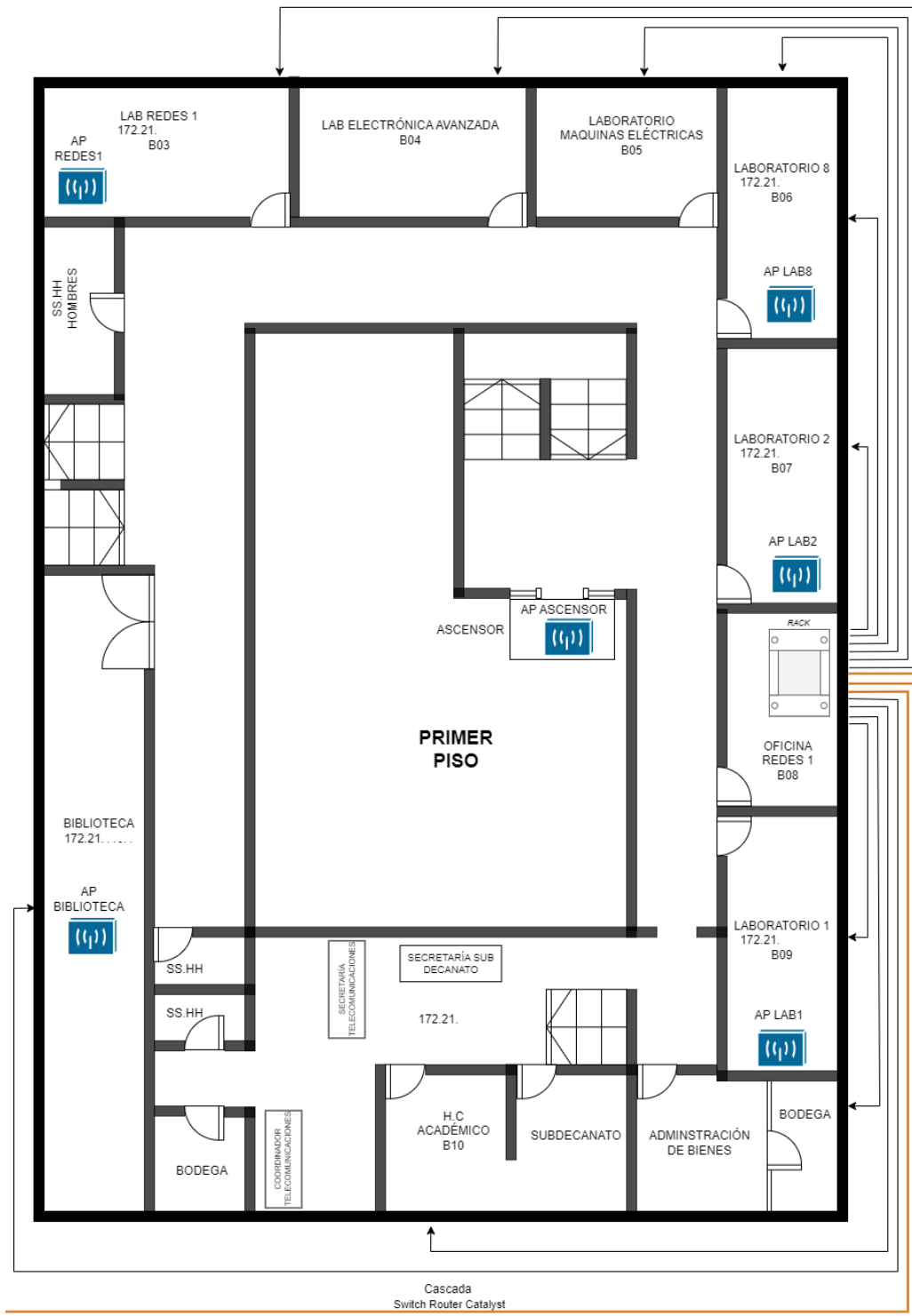
Anexo II

Mapa de red de la Planta baja de la Facultad de Ingeniería en Sistemas Electrónica e Industrial.



Nota. En la imagen se visualiza el mapa de red del Bloque 1 junto con la ubicación de los APs.

Mapa de red del Primer piso de la Facultad de Ingeniería en Sistemas Electrónica e Industrial.



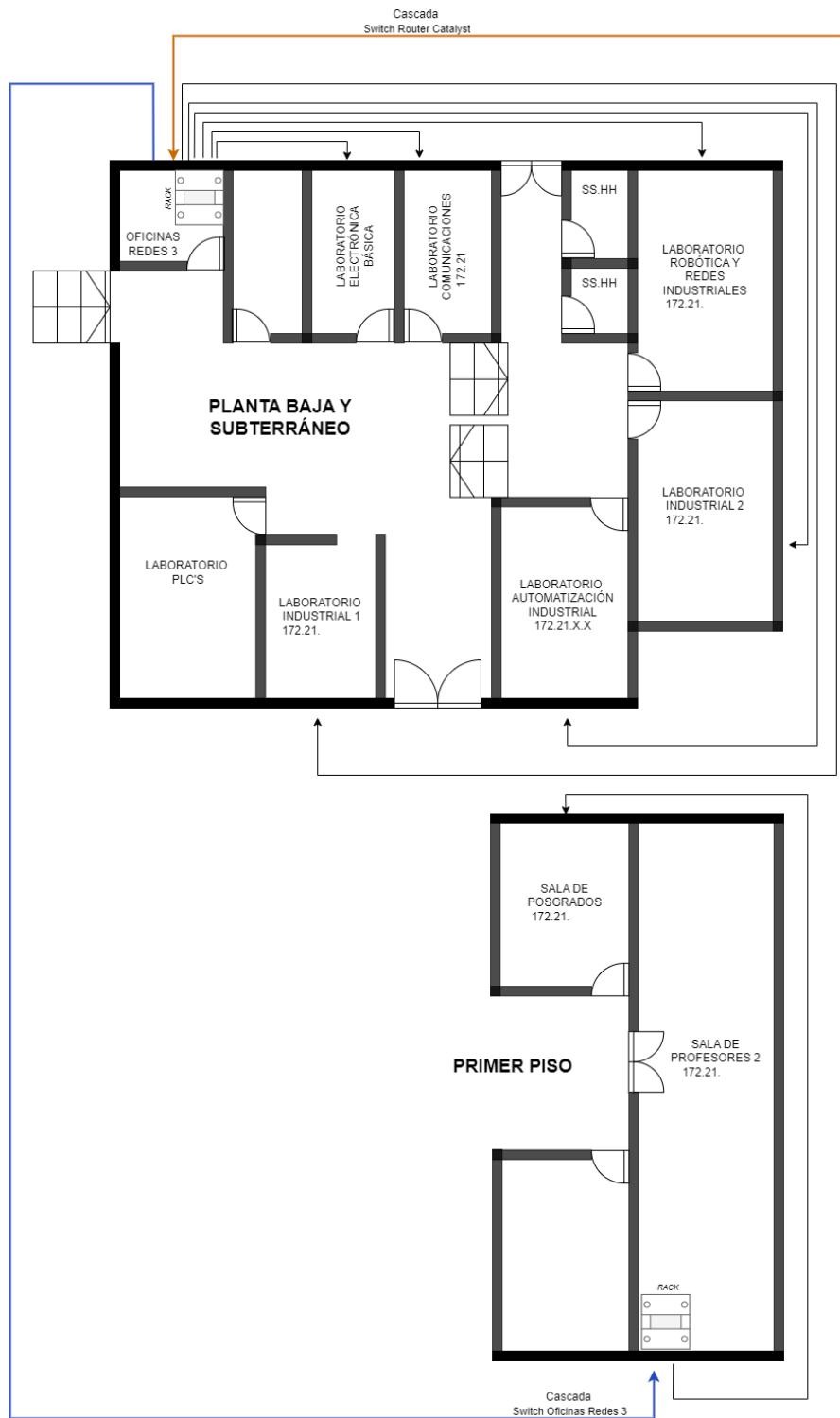
Nota. En la imagen se visualiza el mapa de red del Bloque 1 junto con la ubicación de los APs.

Mapa de red del Segundo piso de la Facultad de Ingeniería en Sistemas Electrónica e Industrial.



Nota. En la imagen se visualiza el mapa de red del Bloque 1 junto con la ubicación de los APs.

Mapa de red de la Planta Baja, Subterráneo y Primer piso del Bloque 2 la Facultad de Ingeniería en Sistemas Electrónica e Industrial



Nota. En la imagen se visualiza el mapa de red del Bloque 1 junto con la ubicación de los APs.

CAPÍTULO VI

PROPUESTA

6. DATOS INFORMATIVOS

6.1. Título

MODELO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN EN LA RED INFORMÁTICA, BASADO EN LA ISO/IEC 27002, CASO DE ESTUDIO UNIVERSIDAD PÚBLICA DEL ECUADOR

6.1.1. Institución

Facultad de Ingeniería en Sistemas, Electrónica e Industrial (FISEI) de la Universidad Técnica de Ambato.

6.1.2. Beneficiarios

Universidad Técnica de Ambato (UTA).

Facultad de Ingeniería en Sistemas, Electrónica e Industrial (FISEI).

Personal Docente y Administrativos.

Estudiantes.

6.1.3. Ubicación

Provincia: Tungurahua

Cantón: Ambato

6.1.4. Técnico responsable

Investigador: Ing. Cristian Javier Saltos Ponce.

Coordinador: Ing. David Omar Guevara Aulestia, Mg.

6.2. Descripción

6.2.1. Antecedentes de la propuesta

Surge de la importancia y necesidad de abordar un enfoque efectivo para proteger los activos de información críticos de una determinada organización, dado a que actualmente enfrentan desafíos contra amenazas cibernéticas que se han ido incrementando significativamente en los últimos años. Esto ha conllevado a un incremento en la adquisición de estándares de seguridad, siendo la norma ISO/IEC 27002, una guía integral para mitigar los riesgos.

6.2.2. Justificación

En un entorno educativo donde la información es un activo crítico, surge la necesidad de establecer buenas prácticas de seguridad de la información. La norma ISO/IEC 27002 se presenta como una estrategia clave para fortalecer la adaptabilidad y la mejora continua en un entorno digital, otorgando la protección integral de los activos de información.

6.2.3. Objetivos

- Determinar la situación actual de la seguridad de la información de la Facultad de Ingeniería en Sistemas Electrónica e Industrial de la Universidad Técnica de Ambato.
- Modelar el sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27002.

6.2.4. Análisis de factibilidad

1. Factibilidad técnica

Se puede mencionar que el proyecto de investigación es técnicamente factible, ya que en la FISEI existen, recursos tecnológicos como es la infraestructura tecnológica (hardware, software, sistemas de información, área de desarrollo y pruebas de proyectos de software, equipos de red).

2. Factibilidad operativa

Operativamente es factible por contar con el recurso humano adecuado y debidamente capacitado en materia de seguridad de la información, para gestionar la continuidad del proyecto.

3. Factibilidad organizativa

Se puede mencionar que organizacionalmente es factible, ya que se cuenta con el consentimiento y aprobación de las autoridades como es Decanato y la Dirección de Tecnología de Información y Comunicación DITIC de la UTA, mismos que muestran interés por disponer de un modelo de gestión para la seguridad de la información, a medida de la FISEI.

4. Factibilidad económica

Desde el punto de vista económico el proyecto es viable ya que no genera, algún tipo de inversión o uso de recursos extras de la institución únicamente consta de trabajo del investigador y la colaboración del personal encargado del departamento de redes, por lo mismo es de gran ayuda para solventar problemas reales en el ámbito social garantizando la concientización de la importancia de estos temas en la actualidad.

5. Fundamentación científica – técnica

La tendencia de ataques cibernéticos genera un aumento de vulnerabilidad donde surgieron diversos grados de impacto lo que obligo a incluir la adopción de medidas de seguridad de la información. La necesidad crítica de proteger los activos de información de una institución, en un entorno cada vez más complejo y propenso a amenazas cibernéticas que se han venido fortaleciendo cada vez más.

Con el pasar del tiempo los ataques informáticos han venido desarrollando nuevas estrategias que se han convertido en formas de ataque a las instituciones tanto públicas como privadas estas pueden ser amenazas externas o internas, por lo que ha llevado a las organizaciones a preocuparse por temas de seguridad de la información, así como su correcta gestión para de esta manera garantizar la continuidad de sus operaciones en caso de que ocurra algún tipo de ataque.

6.3. Desarrollo de la propuesta

PLAN DEL MODELO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (Alcance)

A continuación, se presenta el desarrollo del modelo de Gestión de la Seguridad de la Información, que es bajo un estudio previo es aplicable en el departamento de Administración de Redes de la Facultad de Ingeniería en Sistemas Electrónica e Industrial de la UTA, mismo que se encuentra ubicado en el Campus Huachi, del cantón Ambato. Se debe considerar que las políticas presentadas en este modelo de gestión deben ser de carácter obligatorio para todo el personal del departamento de Administración de Redes de la FISEI.

DECLARACIÓN DE APLICABILIDAD

Es importante considerar la declaración de aplicabilidad conocido como Arquitectura Orientada a Servicios SOA, mismo que corresponde a un documento basado en los

controles de la norma ISO/IEC 27002, el cual es el punto inicial para la aplicación de un modelo SGSI en el departamento de Administración de Redes de la FISEI.

Con la finalidad de identificar y analizar los controles que pueden ser aplicables e implementados en la institución, se realiza un análisis haciendo referencia a la Tabla 20 en la que se puede ver los códigos de estado acorde a su significado según el proceso de madurez que tendrá cada control.

Tabla 20

Selección de controles

Códigos Estado	Significado
D	El control se documentó e implementó
MD	El Control se lleva a cabo y el proceso debe ser documentado para asegurar la respetabilidad del proceso y mitigar los riesgos.
RD	El control no cumple las normas y debe ser rediseñado para cumplir con las normas
PNP	El proceso no está en su lugar / no implementado. (Control requeridos ni documentado ni implementado)
NA (No Aplicable)	El control no es aplicable para la empresa ni para el negocio

Nota. En la tabla se muestra los códigos de estado relacionados a cuál es el nivel que tiene el control de la norma ISO/IEC 27002.

Por lo que se puede describir desde la Tabla 21 a la Tabla 34 el estado de aplicabilidad y cuál es su grado de madurez de los controles de la norma ISO/IEC 27002.

FASE 1: SITUACIÓN ACTUAL.

Tabla 21

Controles referentes a las Políticas de Seguridad, asociados a la Norma ISO/IEC 27002:2013.

5. POLÍTICAS DE SEGURIDAD				
5.1 Directrices de la Dirección en seguridad de la información.				
Control	Descripción	Estado	Hallazgo u Observaciones	Recom

5.1.1	Conjunto de políticas para la seguridad de la información.	PNP	Se observa que actualmente la FISEI no tiene implementado ni documentado sus propios controles, y se rige a las políticas generales de la UTA a la que pertenece, sin embargo, cuenta con políticas internas que deben ser rediseñadas para cumplir con las normas.	Se debe... seguridad... necesidad... acuerdo... previam...
5.1.2	Revisión de las políticas para la seguridad de la información.	PNP	Al no tener documentado sus propios controles, no se realiza en la actualidad una revisión de cumplimiento de forma continua.	Es muy... las polí... de gran... manten... ocurren... informa...

Nota. En la tabla se muestra un conjunto de directrices referentes a las políticas de seguridad asociados a la Norma ISO/IEC 27002.

Tabla 22

Controles referentes a los aspectos organizativos de la seguridad de la información, asociados a la Norma ISO/IEC 27002:2013.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

6.1 Organización interna.

6.1.1	Asignación de responsabilidades para la seguridad de la información.	RD	Actualmente se evidencia que tienen documentado funciones actualizadas con respecto a los roles, pero que no corresponden a la seguridad de la información.	Se debe... respons... de segu... instituc...
6.1.2	Segregación de tareas.	MD	Se evidencia que llevan un control con relación a los accesos indebidos a la información o a las aplicaciones o sistemas que la gestionan (activos de información), pero no se encuentra correctamente documentado.	Es reco... deberes... posibili... informa... uso de l...

6.1.3	Contacto con las autoridades.	MD	No cuentan con documentación actualizada sobre contactos directos con las autoridades que ayuden a suprimir o mitigar una amenaza. Tampoco cuenta con agencias de protección de datos, que velen por el cumplimiento de la seguridad de la información.	Se del apropia solvent la infor sensible
6.1.4	Contacto con grupos de interés especial.	PNP	No tiene contacto con foros, organismos administrativos o entidades expertas en seguridad de la información que le mantenga alerta de las nuevas amenazas que se van actualizando a diario.	Al ser manejar este co especial informa
6.1.5	Seguridad de la información en la gestión de proyectos.	PNP	Se evidencia que la institución no cuenta con el control para establecer un proceso para integrar la Seguridad de la información en cualquier proyecto que se aborde.	Es nec Informa los pro instituc vulnera desarro

6.2 Dispositivos para movilidad y teletrabajo.

6.2.1	Política de uso de dispositivos para movilidad.	PNP	Se evidencia que no se da el manejo adecuado por parte de la institución al no determinar mediante una política las condiciones de uso para estos dispositivos móviles y supervisar el cumplimiento.	Los ries al conec son de desarro estos di
6.2.2	Teletrabajo.	PNP	Actualmente la institución cuenta con la infraestructura tecnológica que le permite migrar tanto al personal administrativo como a clases virtuales a sus estudiantes, pero carece del control que garantice la protección de esta información.	Es muy involuc acceso, a al alc adecuac identifi

Nota. En la tabla se muestra un conjunto aspectos organizativos de la seguridad de la información asociados a la Norma ISO/IEC 27002.

Tabla 23

Controles referentes a la seguridad ligada a los recursos humanos, asociados a la Norma ISO/IEC 27002:2013

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

7.1 Antes de la contratación.

Investigación de antecedentes.	No Aplicable	El área encargada de este control es recursos humanos de la UTA a la que pertenece la FISEI por lo que este control no aplica.	Los nuevos empleados que ingresan deben pasar por un proceso de selección por recursos humanos de la UTA, por lo que este control no aplica.
Términos y condiciones de contratación.	No Aplicable	El área encargada de este control es recursos humanos de la UTA a la que pertenece la FISEI por lo que este control no aplica.	Los nuevos empleados que ingresan deben pasar por un proceso de selección por recursos humanos de la UTA, por lo que este control no aplica.

7.2 Durante la contratación.

Responsabilidades de gestión.	No Aplicable	En el proceso de contratación la UTA da a conocer las políticas internas de la institución.	La UTA como ente de contratación proporciona la información necesaria para asegurar que los empleados cumplan con las responsabilidades en temas de Seguridad de la Información desde su ingreso hasta su retiro.
Concienciación, educación y capacitación en seguridad de la información	PNP	Aunque los empleados conocen sus deberes y responsabilidades, la FISEI a través de una gestión interna refuerza a sus empleados mediante capacitaciones, para un mejor desempeño laboral, pero no cuenta con el control requerido por la normativa.	La FISEI a través de la UTA y sus áreas debe establecer programas permanentes para fomentar una cultura informática en temas de seguridad de la información para los empleados, capacitándolos constantemente.
Proceso disciplinario.	No Aplicable	Actualmente el incumplimiento de políticas o falta grave está sujeta a un proceso disciplinario por parte de recursos humanos de la UTA.	Los empleados deben tener en cuenta los procesos disciplinarios por parte de recursos humanos de la UTA, por lo que este control no aplica.

7.3 Cese o cambio de puesto de trabajo.

Cese o cambio de puesto de trabajo.	No Aplicable	El área encargada de este control es recursos humanos de la UTA a la que pertenece la FISEI por lo que este control no aplica.	Los nuevos empleados que ingresan deben pasar por un proceso de selección por recursos humanos de la UTA, por lo que este control no aplica.
--	---------------------	--	--

Nota. En la tabla se muestra un conjunto de aspectos organizativos de la seguridad de la información asociados a la Norma ISO/IEC 27002.

Tabla 24

Controles referentes a la gestión de activos, asociados a la Norma ISO/IEC 27002:2013.

8. GESTIÓN DE ACTIVOS

8.1 Responsabilidad sobre los activos.

Inventario de activos.	RD	Actualmente la FISEI cuenta con un área de bienes encargada de llevar el inventario físico de los recursos de la institución, pero no cuenta con un área especializada en realizar un inventario de activos de la información.	Se debe tratar de mantener un inventario de activos de información que permita el control de la información basados en su sensibilidad, riesgo de pérdida, y el propietario y responsable del activo.
Propiedad de los activos.	RD	Actualmente no se cuenta con un área especializada encargada de llevar el inventario de activos de tecnología e información y su respectivo control.	Se debe gestionar un área responsable de mantenimiento y control de tecnología e información, incluyendo el licenciamiento de software donde se establezcan las responsabilidades.
Uso aceptable de los activos.	PNP	Se puede evidenciar que para el personal no está clara la clasificación de activos para uso indebido de seguridad de la información.	Documentar y socializar el uso aceptable de la información, empezando por los responsables de los activos de información para evitar el uso indebido.
Devolución de activos.	RD	Actualmente para la desvinculación o retiro de personal existe un acta de entrega de bienes, donde se entrega los activos físicos que se encontraban bajo la responsabilidad de esta persona, pero no cuentan con el control de entrega de activos de información.	Se debe contar de manera clara y oportuna el control al ser de gran importancia para los activos de información una vez finaliza la contratación del personal incluyendo la devolución de información de forma segura y controlada cuando sea necesario.

8.2 Clasificación de la información.

Directrices de clasificación.	PNP	No se cumple con este control, por lo que es necesario considerar que el responsable del activo es quien clasifica la información.	Los dueños de la información son responsables de velar por la seguridad de la información clasificándola por niveles de criticidad, la confidencialidad, estos detalles se establecen en las políticas de seguridad.
Etiquetado y manipulado de la información.	PNP	Actualmente el departamento de bienes etiqueta los activos físicos de la institución, en cuanto a los activos de la información no se llevan un etiquetado que permita clasificar la información en crítica y sensible.	Se debe desarrollar el proceso de etiquetado adecuado por parte de los dueños de la información especificando los niveles de sensibilidad de la misma.
Manipulación de activos.	PNP	Este control no se cumple, en cada área que genera información generando riesgos por pérdida de la misma por falta de un correcto inventario de activos de información.	Se debe socializar con cada directiva de la institución, para que proceda a establecer los procedimientos para el manejo de la información consideren la clasificación de la información.

8.3 Manejo de los soportes de almacenamiento.

Gestión de soportes extraíbles.	PNP	Se puede evidenciar que no se cuenta con el cumplimiento de este control que gestione los soportes extraíbles y hagan cumplir con la seguridad necesaria.	Se debería controlar la transferencia de información hacia medios extraíbles, de uso personal de los funcionarios, sin la debida autorización inmediata y de la Administración.
--	------------	---	---

Eliminación de soportes.	PNP	No se cuenta con un control para establecer procedimientos para la eliminación segura de información sensible de equipos extraíbles que no permitan la recuperación de la misma.	Las copias de seguridad y respaldos permanentes, considerando la información confidencial contenida en los dispositivos de la institución. Se debe establecer un procedimiento para la eliminación y finalización de su uso.
Soportes físicos en tránsito.	No Aplicable	Este control no aplica ya que la FISEI no necesita trasladar la información a otras ubicaciones.	Este control no aplica ya que la FISEI no necesita trasladar la información a otras ubicaciones.

Nota. En la tabla se muestra los controles referentes a la gestión de activos asociados a la Norma ISO/IEC 27002.

Tabla 25

Controles referentes al control de accesos., asociados a la Norma ISO/IEC 27002:2013.

9. CONTROL DE ACCESOS				
9.1 Requisitos de negocio para el control de accesos.				
9.1.1	Política de control de accesos.	PNP	Se evidencia que no se encontró documentación sobre las reglas que rigen el proceso de permisos a cuentas de usuarios con altos privilegios y documentación de roles para visualizar determinados contenidos.	Se debe implementar una política de control de accesos para el control de documentos para el control de accesos.
9.1.2	Control de acceso a las redes y servicios asociados.	RD	Este control no se encuentra totalmente completo, no se evidencia una matriz de usuarios con sus respectivos privilegios. Sin embargo, existen perfiles de usuario y acceso a distintas aplicaciones, pero no se la documenta.	El control de acceso a las redes y servicios asociados debe ser controlado de manera distinta.
9.2 Gestión de acceso de usuario.				
9.2.1	Gestión de altas/bajas en el registro de usuarios.	PNP	Este control en la actualidad no se cumple, ya que no se gestiona el control de altas/bajas en el registro de usuarios.	Se sugiere implementar un control de acceso de usuarios y abandonar el control de accesos.
9.2.2	Gestión de los derechos de acceso asignados a usuarios.	PNP	Se evidencia que los departamentos de la institución no tienen documentado un proceso formal a cada una de las aplicaciones. Carece de un método para asignar y revocar los accesos a los diferentes servicios.	Se debe implementar un control de acceso de usuarios al acceso de servicios de información confidencial.

9.2.3	Gestión de los derechos de acceso con privilegios especiales.	PNP	En la institución se maneja sistemas de información, sin embargo no se ha llegado a documentar las restricciones que tendrán los usuarios en cuanto a su acceso.	La institución maneja sistemas de información, sin embargo no se ha llegado a documentar las restricciones que tendrán los usuarios en cuanto a su acceso.
9.2.4	Gestión de información confidencial de autenticación de usuarios.	PNP	No se evidencia procesos que garanticen la confidencialidad de autenticación de usuarios, se debe incluir cláusulas y condiciones sobre el mantenimiento secreto de contraseñas.	Los usuarios deben tener acceso a la información confidencial de autenticación de usuarios.
9.2.5	Revisión de los derechos de acceso de los usuarios.	PNP	Este control no se cumple porque actúa con políticas existentes referentes a los accesos de los usuarios haciendo una revisión periódica de los permisos.	Se debe hacer una revisión periódica de los permisos de los usuarios para detectar cualquier cambio.
9.2.6	Retirada o adaptación de los derechos de acceso	PNP	Este control no se cumple porque actúa con políticas existentes mismo exige mantener el seguimiento a las políticas ya implementadas.	Es necesario que se retire o adapte los derechos de acceso de los usuarios cuando sea necesario de manera definitiva.

9.3 Responsabilidades del usuario.

9.3.1	Uso de información confidencial para la autenticación.	PNP	Este control no se cumple porque actúa con políticas existentes referentes a los accesos de los usuarios haciendo una revisión periódica de los permisos.	Se debe hacer una revisión periódica de los permisos de los usuarios para detectar cualquier cambio.
-------	--	-----	---	--

9.4 Control de acceso a sistemas y aplicaciones.

9.4.1	Restricción del acceso a la información.	PNP	En la institución se maneja sistemas de información, sin embargo, no se ha llegado a documentar las restricciones que tendrán los usuarios en cuanto a su acceso.	La institución maneja sistemas de información, sin embargo, no se ha llegado a documentar las restricciones que tendrán los usuarios en cuanto a su acceso.
9.4.2	Procedimientos seguros de inicio de sesión.	RD	La institución gestiona cursos para mejorar el buen rendimiento del personal en sus actividades, pero debe enfocar las capacitaciones en temas de seguridad de la información.	Los usuarios deben tener acceso a la información confidencial de autenticación de usuarios.

9.4.3	Gestión de contraseñas de usuario.	PNP	Se evidencia que la política no se encuentra establecida con los lineamientos a tener en cuenta en la definición de contraseñas.	<ul style="list-style-type: none"> • Tiene palabras de diccionario como contraseña. • Al menos una letra en minúscula. • Debe ser de al menos 8 caracteres. • No debe contener espacios. • No debe ser idéntica a la primera letra.
9.4.4	Uso de herramientas de administración de sistemas.	PNP	Este control de monitoreo de la actividad de los usuarios administradores, no se encuentra implementado en el área de Administración de Redes y no está documentado.	El departamento de Administración de Redes no tiene un procedimiento por escrito que describa las condiciones de monitoreo de la actividad de los usuarios administradores en las plataformas de administración de sistemas.
9.4.5	Control de acceso al código fuente de los programas.	D	Este control no se encuentra implementado en el departamento de Administración de Redes y no se encuentra documentado acorde a la normativa.	El departamento de Administración de Redes no tiene un procedimiento por escrito que describa las condiciones de acceso al código fuente de los programas.

Nota. En la tabla se muestra los controles de accesos asociados a la Norma ISO/IEC 27002.

Tabla 26

Controles referentes al cifrado., asociados a la Norma ISO/IEC 27002:2013

10. CIFRADO

10.1 Controles criptográficos.

Política de uso de los controles criptográficos.	PNP	Este control no se encuentra implementado en el departamento de Administración de Redes y no se encuentra documentado acorde a la normativa.	La institución deberá asegurar que la información clasificada como restringida e información sensible no sea transmitida por cualquier medio durante el almacenamiento o la transmisión para proteger su confidencialidad e integridad.
Gestión de claves.	PNP	Este control no se encuentra implementado en el departamento de Administración de Redes y no se encuentra documentado acorde a la normativa.	Los dispositivos deben ser propiedad del departamento de Administración de Redes de la institución, gestionados a través de un procedimiento por escrito.

Nota. En la tabla se muestra un conjunto de controles referentes al cifrado, asociados a la Norma ISO/IEC 27002:2013.

Tabla 27

Controles referentes a la seguridad física y ambiental, asociados a la Norma ISO/IEC 27002:2013.

11. SEGURIDAD FÍSICA Y AMBIENTAL				
11.1 Áreas seguras.				
11.1.1	Perímetro de seguridad física.	RD	Claramente, se necesitan controles de protección para brindar seguridad física alrededor de las instalaciones que albergan el equipo informático para restringir el personal no autorizado.	Se re centrán control
11.1.2	Controles físicos de entrada.	RD	Actualmente cada una de las áreas cuenta con acceso a cada uno de sus funcionarios previamente identificados, permitiendo tener un control efectivo en los accesos del personal.	Todos l deberán de la in
11.1.3	Seguridad de oficinas, despachos y recursos.	MD	Actualmente, todos los funcionarios pres identificados se encuentran ubicados en cada zona a la que corresponde, lo que permite un control efectivo del acceso del personal, pero hace falta documentar de manera correcta este control.	Se debe desde la lo que cumplir realizad
11.1.4	Protección contra las amenazas externas y ambientales.	MD	Actualmente se siguen una serie de reglas necesarias, pero falta socializar, para respetar la seguridad de los recursos físicos, sin embargo, en algunos casos existe incumplimiento de las normas, por lo que es necesario desarrollar cursos para fortalecer la seguridad de la información.	La insti físicas y protecc recursos ubicada con sist detecció evacuac

11.1.5	El trabajo en áreas seguras.	D	Actualmente, cada área cuenta con las oportunidades de desarrollo adecuadas, teniendo en cuenta los controles que le permitan funcionar adecuadamente, garantizando la seguridad y protección del grupo de trabajo.	La inst efectivi control instalac
11.1.6	Áreas de acceso público, carga y descarga.	No Aplicable	No aplica	No apli
11.2 Seguridad de los equipos.				
11.2.1	Emplazamiento y protección de equipos.	MD	Actualmente se siguen las políticas necesarias para garantizar la seguridad de los recursos materiales por motivos medioambientales. Sin embargo, en algunos casos existe exceso de confianza e incumplimiento de la política interna, por lo que es necesario realizar cursos de capacitación para fortalecer el tema.	Los rec de Red físicame autORIZA exposic interrup
11.2.2	Instalaciones de suministro.	D	Actualmente, este control se logra a través de una red mantenida periódicamente que permite alertas de emergencia, así como soporte preventivo para evitar daños mayores. El responsable de este control se lleva a través de políticas la institución.	La inst manten sean m debidam importa manten
11.2.3	Seguridad del cableado.	D	Actualmente, este control se logra a través de una red mantenida periódicamente que permite alertas de emergencia, así como soporte preventivo para evitar daños mayores.	El área que los bajo su líquidos incendi
11.2.4	Mantenimiento de los equipos.	MD	Actualmente este control se encuentra implementado a través de políticas de mantenimiento periódico que permite alertar en caso de emergencia y adicional dar un soporte preventivo para evitar futuros daños.	Los me informa y lógic condici manten meses necesari
11.2.5	Salida de activos fuera de las dependencias de la empresa.	RD	Actualmente no se lleva un registro de préstamos de salidas de diversos equipos fuera de la institución, solo préstamos internos.	La insti préstam trabajo, informa por el p
11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	No Aplicable	No aplica	No apli

11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.	RD	No se cuenta con protocolos de seguridad que permiten controlar el movimiento de equipos informáticos, es importante implementar protocolos para evitar futuros inconvenientes.	Los de utilizar tecnología segura informática cambio
11.2.8	Equipo informático de usuario desatendido.	RD	El acceso remoto a las estaciones de trabajo no está permitido en la UTA a la que pertenece la FISEI, pero dado a la necesidad del personal administrativo y bajo la autorización de facultad tienen implementado control de accesos a estaciones de trabajo pero esta información no la tienen documentada.	El depa trabajar quienes el corre dentro y informa autoriza
11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla.	PNP	Este control no se encuentra implementado en el área de Administración de Redes acorde a la normatividad solicitada.	Los fun terceros al llega docume desemp

Nota. En la tabla se muestra un conjunto de controles referentes a la seguridad física y ambiental, asociados a la Norma ISO/IEC 27002.

Tabla 28

Controles referentes al control de seguridad en la operativa, asociados a la Norma ISO/IEC 27002:2013

12. SEGURIDAD EN LA OPERATIVA

12.1 Responsabilidades y procedimientos de operación.

12.1.1	Documentación de procedimientos de operación.	RD	El departamento de Administración de Redes en la actualidad no cuenta documentado la información relacionada con la administración de los sistemas informáticos, manuales, procedimientos y políticas que permiten que este control se encuentre de forma adecuada dentro de la institución.	El depa tener un sobre p manejo solución
--------	--	-----------	--	--

12.1.2	Gestión de cambios.	PNP	Es importante llevar un control de cambios efectivo, ya que en algunas reuniones se evidencia que hay información que no se documenta o no queda registrada de forma completa en los controles de cambio.	Se debe seguridad obligaci virus.
12.1.3	Gestión de capacidades.	PNP	Se evidencia que no se considera el tema relacionado a pérdidas de disponibilidad o rendimiento relacionadas a la falta de capacidad del personal.	Se debe relación ampliación capacidad
12.1.4	Separación de entornos de desarrollo, prueba y producción.	PNP	Se evidencia que la FISEI no cuenta con un entorno para el desarrollo de código fuente, aplicaciones y pruebas.	La insti y neces desarrollo mejor d contar c
12.2 Protección contra código malicioso.				
12.2.1	Controles contra el código malicioso.	MD	Se evidencia que existe falta de conocimiento del propio personal ya que deben estar preparados y saber responder ante ataques contra la seguridad de la información. La institución cuenta con un antivirus que ayuda en los puestos de trabajo, pero no se dispone uno en el servidor.	La insti de códi, como e totalme
12.3 Copias de seguridad.				
12.3.1	Copias de seguridad de la información.	D	Las copias de seguridad no son realizadas por parte del departamento de Administración de Redes, no se cuenta con políticas de copias de seguridad o respaldo de la información que cuente con la periodicidad con las que se deberían hacer.	La insti seguridad la frecu
12.4 Registro de actividad y supervisión.				
12.4.1	Registro y gestión de eventos de actividad.	RD	El departamento de Administración de Redes cuenta con un monitoreo continuo con la herramienta Notion donde pueden monitorizar el funcionamiento y eventos que surgen a diario.	Este continu los recu funcion terceros
12.4.2	Protección de los registros de información.	PNP	Actualmente el departamento de Redes no cuenta con una protección apropiada contra los registros de eventos, considerando los cambios y corrupción de información no autorizados.	El regis donde p para bo también

12.4.3	Registros de actividad del administrador y operador del sistema.	PNP	Monitorear los eventos que ocurren en el sistema, para evitar fugas de información es muy importante fortalecer la seguridad de la información en el grupo de trabajo.	El área periódicamente administra tecnología, identifica actividades
12.4.4	Sincronización de relojes.	PNP	Anteriormente se evidenció que no se lleva un registro correcto de eventos, mismo que se hace con la herramienta Notion, esta aplicación se sincroniza con la zona horaria donde se esté abriendo la aplicación Notion.	La institución sincroniza procesos de la entidad
12.5 Control del software en explotación.				
12.5.1	Instalación del software en sistemas en producción.	D	Este control actualmente se encuentra funcionando de forma correcta.	Deberá controlarse dispositivos tener el
12.6 Gestión de la vulnerabilidad técnica.				
12.6.1	Gestión de las vulnerabilidades técnicas.	D	Este control actualmente se encuentra funcionando. Sin embargo, se evidencia que en algunos casos no se cumple, existen equipos informáticos que no cuentan con las respectivas actualizaciones del software dando paso a vulnerabilidades que puedan ser aprovechadas por los atacantes.	La organización aparición recursos pruebas
12.6.2	Restricciones en la instalación de software.	D	En la institución, es importante considerar el perfil y rol de cada usuario al momento de instalar aplicaciones. Sin embargo, existen equipos que no cuentan con las medidas de seguridad para que no se instalen aplicaciones sin autorización.	La institución suministra exclusividad Informa
12.7 Consideraciones de las auditorías de los sistemas de información.				
12.7.1	Controles de auditoría de los sistemas de información.	PNP	Falta de monitoreo en los eventos que ocurren en el sistema, para evitar fugas de información es muy importante fortalecer la seguridad de la información en el grupo de trabajo.	El canal constante política implementado estado informa

Nota. En la tabla se muestra un conjunto de controles referentes a la seguridad en la operativa, asociados a la Norma ISO/IEC 27002.

Tabla 29

Controles referentes a la seguridad en las telecomunicaciones, asociados a la Norma ISO/IEC 27002:2013

13. SEGURIDAD EN LAS TELECOMUNICACIONES			
13.1 Gestión de la seguridad en las redes.			
Controles de red.	PNP	Se puede evidenciar que no se cuenta con una gestión que controle la red dentro de la institución, el soporte sobre todos los dispositivos que interconectan al exterior.	La institución debe establecer control necesarios para dar soporte los equipos (routers, switch, etc.), consideren la seguridad inalámbrica.
Mecanismos de seguridad asociados a servicios en red.	MD	El acceso a varios sitios web está controlado en la institución, pero el acceso es posible sin restricciones en algunas máquinas de la institución.	Los mecanismos de seguridad y servicio de red deben definirse nivel servicio. Debe tener visibilidad disponibilidad de la red, ya que es el buen funcionamiento de la información de la institución.
Separación de redes.	No Aplicable	No aplica	No aplica
13.2 Intercambio de información con partes externas.			
Políticas y procedimientos de intercambio de información.	MD	Se evidencia que la información enviada internamente no cuenta con políticas ni documentación para proteger la información.	Se recomienda tener en cuenta medios de transmisión, las redes, s
Acuerdos de intercambio.	No Aplicable	No se envía información física o en dispositivos electrónicos fuera de la institución.	No se envía información física o electrónicos fuera de la institución
Mensajería electrónica.	PNP	Toda información enviada a través de mensajería electrónica, así como mensajería por redes sociales debe asegurarse de la protección de la confidencialidad de los datos.	La institución debe darle la importancia de correo electrónico como herramienta la comunicación entre funcionarios brindará un servicio ideal y actividades que requieran el electrónico, respetando siempre la integridad, disponibilidad.
Acuerdos de confidencialidad y secreto.	No Aplicable	Este control no aplica por estar enfocado en la seguridad entre clientes y proveedores.	Este control no aplica por estar seguridad entre clientes y proveed

Nota. En la tabla se muestra controles referentes a la seguridad en las telecomunicaciones, asociados a la Norma ISO/IEC 27002.

Tabla 30

Controles referentes la adquisición, desarrollo y mantenimiento de los sistemas de información, asociados a la Norma ISO/IEC 27002:2013.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE I				
14.1 Requisitos de seguridad de los sistemas de información.				
14.1.1	Análisis y especificación de los requisitos de seguridad.	No Aplicable	Se enfoca en requisitos para la seguridad de las funcionalidades antes de su fase de desarrollo.	Se enfo
14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas.	PNP	El acceso a los distintos medios de la institución deberá realizarse de forma segura de manera interna y con el permiso correspondiente.	El área que los informá seguridad la infor disposit
14.1.3	Protección de las transacciones por redes telemáticas.	No Aplicable	No aplica	No apli
14.2 Seguridad en los procesos de desarrollo y soporte.				
14.2.1	Política de desarrollo seguro de software.	No Aplicable	No aplica	No apli
14.2.2	Procedimientos de control de cambios en los sistemas.	No Aplicable	Control enfocado a la vigilancia y control de actualizaciones de sistemas operativos y navegadores.	Control actualiz navegac
14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	No Aplicable	Control enfocado en la revisión de las aplicaciones luego de una actualización.	Control luego d

14.2.4	Restricciones a los cambios en los paquetes de software.	PNP	Control enfocado en limitar las actualizaciones sobre determinado software adquirido, considerando cambios absolutamente necesarios.	Realiza proporc requisit riesgo l
14.2.5	Uso de principios de ingeniería en protección de sistemas.	No Aplicable	Control enfocado en documentar procedimientos seguros para el desarrollo de sistemas informáticos, en la institución netamente no desarrolla Software.	Control seguros en la in
14.2.6	Seguridad en entornos de desarrollo.	No Aplicable	No desarrollan código para la creación de sistemas.	No desa
14.2.7	Externalización del desarrollo de software.	No Aplicable	En la actualidad el desarrollo de aplicaciones es realizado por la DITIC, perteneciente a la UTA.	En la a realizad
14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas.	No Aplicable	En la actualidad el desarrollo de aplicaciones es realizado por la DITIC, perteneciente a la UTA.	En la a realizad
14.2.9	Pruebas de aceptación.	No Aplicable	En la actualidad el desarrollo de aplicaciones es realizado por la DITIC, perteneciente a la UTA.	En la a realizad
14.3 Datos de prueba.				
14.3.1	Protección de los datos utilizados en pruebas.	No Aplicable	En la actualidad el desarrollo de aplicaciones es realizado por la DITIC, perteneciente a la UTA.	En la a realizad

Nota. En la tabla se muestra un conjunto controles referentes la adquisición, desarrollo y mantenimiento de los sistemas de información, asociados a la Norma ISO/IEC 27002.

Tabla 31

15. RELACIONES CON SUMINISTRADORES				
15.1 Seguridad de la información en las relaciones con suministradores.				
15.1.1	Política de seguridad de la información para suministradores.	D	Todos los proveedores, vendedores o prestadores de servicios de la institución tienen sus propias políticas de seguridad de la información, pero es importante recordarlas periódicamente.	La institución sus relaciones de información presta procedimientos
15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores.	MD	Todos los proveedores, vendedores o prestadores de servicios de la institución tienen sus propias políticas de seguridad de la información, pero es importante recordarlas periódicamente.	Se debe de nivel de información seguridad
15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones.	D	Los proveedores se contratan sobre una base competitiva para garantizar los proveedores de alta calidad que satisfagan las necesidades de la institución.	Se debe de confidencialidad de información y de seguridad
15.2 Gestión de la prestación del servicio por suministradores.				
15.2.1	Supervisión y revisión de los servicios prestados por terceros.	D	Establezca un mecanismo de auditoría para sus proveedores de servicios para garantizar el pleno cumplimiento del acuerdo de servicio.	El departamento identifica a terceros actividades de los servicios prestados
15.2.2	Gestión de cambios en los servicios prestados por terceros.	MD	La modificación de los servicios prestados según proveedor se realiza en la institución considerando los controles de cambios, el cual está organizado por las distintas áreas receptoras del servicio. Hace falta tener el sustento de un área de seguridad de la información.	Los equipos de apoyo de mantenimiento de seguridad de nuevos

Nota. En la tabla se muestra un conjunto de controles referentes las relaciones con suministradores, asociados a la Norma ISO/IEC 27002.

Tabla 32

Controles referentes la gestión de incidentes en la seguridad de la información., asociados a la Norma ISO/IEC 27002:2013.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN			
16.1 Gestión de incidentes de seguridad de la información y mejoras.			
Responsabilidades y procedimientos.	PNP	Se evidencia la falta de un responsable de cumplimiento adecuado y definir procedimientos que dirijan a la etapa de incidentes de seguridad de la información en la institución.	La institución facilitará la denuncia de terceros funcionarios y personas relacionados con la seguridad de la información en las formas en que se maneja, incluido el tipo de medio como plataformas de sistemas de información, medios f
Notificación de los eventos de seguridad de la información.	PNP	Se evidencia que el personal no está totalmente capacitado para tales situaciones, pero es importante recalcarle la importancia de informar periódicamente los incidentes que puedan afectar la seguridad de la información, ya que en algunos casos no informarán estos incidentes.	Los propietarios de activos de información deben notificar inmediatamente al Departamento de Administración de Redes cualquier incidente de seguridad que descubran o conozcan.
Notificación de puntos débiles de la seguridad.	RD	El personal está parcialmente capacitado para tales situaciones, pero es importante recalcarle la importancia de informar periódicamente los incidentes que puedan afectar la seguridad de la información, ya que en algunos casos no informarán estos incidentes.	Si los funcionarios descubren que información interna, reservada o restringida ha sido divulgada sin autorización, debe ser reportada al Departamento de Administración de Redes para que pueda ser registrada y procesada de acuerdo al procedimiento necesario.
Valoración de eventos de seguridad de la información y toma de decisiones.	RD	Las actividades de seguridad se llevan parcialmente a cabo en el área de Administración de Redes para su respectiva solución, sin embargo, hace falta que lleven un análisis de impacto de cualquier desarrollo que amenace la seguridad de la información.	El departamento de Administración de Redes debe considerar tener un Comité de Seguridad de la Información donde se deberá analizar los incidentes de seguridad que se le comuniquen y se inicien procedimientos de cooperación con las autoridades.
Respuesta a los incidentes de seguridad.	PNP	La respuesta que se brinda es básica no efectiva y no se realiza seguimiento continuo en cuanto si ocurre un ataque informático.	La seguridad de la información requiere personal calificado para investigar a fondo los incidentes de seguridad reportados, identificar la causa de las investigaciones exhaustivas, brindar soluciones en última instancia, evitar que vuelvan a ocurrir.

Aprendizaje de los incidentes de seguridad de la información.	PNP	Todos los incidentes de seguridad de la información son parcialmente reportados en los diferentes departamentos, se debería capacitar de mejor manera al personal con la finalidad de evitar que incidentes de seguridad se repitan.	Considerar crear un área de información, con el apoyo del área de autoridades de la institución, y con los conocimientos y proponer soluciones a los incidentes de seguridad, de modo que en esta base de conocimientos, se rediseñe la respuesta ante futuros incidentes.
Recopilación de evidencias.	PNP	En cada caso, son pocos los casos que se recopilan las pruebas necesarias para garantizar la seguridad de la información y mantener la trazabilidad total de cada caso.	Es importante evaluar todos los incidentes de seguridad caso por caso, reunir la evidencia necesaria y considerarlos como evidencia para tener documentado en el departamento de seguridad.

Nota. En la tabla se muestra un conjunto de controles referentes a la gestión de incidentes en la seguridad de la información, asociados a la Norma ISO/IEC 27002.

Tabla 33

Controles referentes a los aspectos de seguridad de la información en la gestión de la continuidad del negocio, asociados a la Norma ISO/IEC 27002:2013

17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

17.1 Continuidad de la seguridad de la información.

Planificación de la continuidad de la seguridad de la información.	PNP	Este control físico no está soportado en la institución y no cuenta con servidores de respaldo para el manejo de la información para garantizar la continuidad del negocio.	Los procedimientos deben documentarse, implementarse periódicamente para garantizar una recuperación razonable y oportuna de la información en un dispositivo sin comprometer el nivel de seguridad establecido.
Implantación de la continuidad de la seguridad de la información.	PNP	Este control físico no está soportado en la institución y no cuenta con servidores de respaldo para el manejo de la información para garantizar la continuidad del negocio.	Se deben proporcionar recursos adecuados a los funcionarios y los procesos pueden ser implementados de manera efectiva cuando ocurra un evento inesperado o catastrófico dentro de la institución que afecte su continuidad comercial.
Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	PNP	Es importante reforzar cómo el personal administrativo, docentes y estudiantes manejen una emergencia o una situación que afecte la continuidad de las actividades académicas.	Debe asegurarse de que los planes de continuidad ante desastres y/o continuidad de operaciones se prueben periódicamente para verificar la efectividad de la información implementada y que estén documentadas.

17.2 Redundancias.

Disponibilidad de instalaciones para el procesamiento de la información.	D	La institución no cuenta con oficinas principales fuera de la institución que brinde soporte tanto a nivel nacional como internacional cuando sea necesario.	Se debe fomentar la existencia de tecnologías redundantes que cumplan con niveles de accesibilidad aceptables.
---	----------	--	--

Nota. En la tabla se muestra un conjunto de controles referentes a los aspectos de seguridad de la información en la gestión de la continuidad del negocio., asociados a la Norma ISO/IEC 27002

Tabla 34

Controles referentes al cumplimiento., asociados a la Norma ISO/IEC 27002:2013.

18. CUMPLIMIENTO			
18.1 Cumplimiento de los requisitos legales y contractuales.			
Identificación de la legislación aplicable.	MD	La FISEI debe esforzarse por cumplir con las regulaciones aplicables y con referencia al sistema en el que opera el personal administrativo y al entorno institucional.	La parte tecnológica debe identificar que el software instalado en la plataforma tecnológica cumpla con las leyes y de licencia aplicables.
Derechos de propiedad intelectual (DPI).	MD	Los derechos de propiedad y derechos de autor sobre todo lo que se realiza en su entorno laboral se ejercen en el marco del contrato establecido por la empresa.	Es importante que todos los dispositivos recuerden que deben cumplir con las leyes de derechos de autor y los acuerdos de software.
Protección de los registros de la organización.	PNP	Hoy en día, el departamento de Administración de Redes no monitorea continuamente las aplicaciones para rastrear posibles incidentes de seguridad de la información. Sin embargo, es importante empezar con capacitar al personal para reducir los riesgos.	Los campos legal y de seguridad de la información deben identificar, documentar y monitorear continuamente los requisitos legales y contractuales que se aplican a la información para protegerlas contra pérdida, falsificación, acceso y divulgación no autorizada.
Protección de datos y privacidad de la información personal.	PNP	Aunque existen políticas internas en relación con el procesamiento de datos personales, es importante dejar claro que cualquiera que quiera utilizar los datos de determinado personal debe estar autorizado hacerlo por el dueño de la información.	De conformidad con las disposiciones de protección de datos personales, la institución debe implementar medidas de protección de los datos personales de los empleados, utilizando el área de información y de gestión que se debe tener en cuenta.
Regulación de los controles criptográficos.	PNP	Este control no se encuentra implementado en el ámbito informático y no funciona según las normas requeridas.	La institución debe implementar controles de cifrado necesarios para proteger la información personal de los destinatarios, proveedores u otros terceros almacenada en un Repositorio o cualquier otro repositorio, evitando su divulgación sin la autorización correspondiente.
18.2 Revisiones de la seguridad de la información.			

Revisión independiente de la seguridad de la información.	RD	Cada departamento es responsable de velar por la seguridad de la información y garantizar que la misma no se vea comprometida, así como informar los incidentes de seguridad que se presenten.	Las entidades deben realizar revisiones para verificar que se requieran políticas de seguridad. Los controles deben cumplir con la norma de seguridad ISO 27001 y otras fuentes (ITIL, BASEL II, etc.).
Cumplimiento de las políticas y normas de seguridad.	PNP	Si bien estas políticas son importantes, no se aplican al procesamiento de datos personales, se debe dejar claro que cualquier persona que no reciba el soporte de seguridad de la información necesario dentro de la empresa podría no poder cumplir con las políticas y estándares establecidos.	Los diversos aspectos del documento de seguridad actualizado deben ser conocidos por todos los funcionarios del personal contratistas y otros asociados.
Comprobación del cumplimiento.	PNP	Confirmar el cumplimiento de las políticas de seguridad establecidas a través de auditorías no anunciadas de cada área y sus procesos y retroalimentar las no conformidades identificadas en el proceso. Es importante recordar que los empleados no sólo deben cumplir con la política de auditoría, sino también desempeñar parte de sus responsabilidades como directivos de la institución	El área de control interno debe revisar periódicamente los registros de plataformas tecnológicas y sistemas para determinar si la información cumple con las políticas y estándares.

Nota. En la tabla se muestra un conjunto de controles referentes al cumplimiento, asociados a la Norma ISO/IEC 27002.

En la Figura 12, se muestra el resultado del estado inicial del nivel de madurez de la FISEI, mientras que la Figura 13 muestra un resumen general de vulnerabilidades aplicando la norma ISO/IEC 27002.

Figura 12

Estado Adecuación Implementación ISO/IEC 27002 vs Objetivos de Control

Etapa de Determinación de la ISO 27002 - Controles					
Referencia	Proceso Cumple con la norma y esta documentado	Proceso se lleva a cabo y se debe documentar	Proceso no cumple con la norma y debe ser rediseñado	Proceso no está en su lugar / no esta implementado	Proceso no es aplicable
ISO Controles	12	13	16	51	22

Estado Adecuación Implementación ISO 27002 vs Objetivos de Control			
ISO/IEC 27002:2013 Objetivos de Control		Cantidad	Conformidad
5.	POLITICAS DE SEGURIDAD.	0	0%
6.	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.	0	0%
7.	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	0	0%
8.	GESTIÓN DE ACTIVOS.	0	0%
9.	CONTROL DE ACCESOS.	1	7%
10.	CIFRADO.	0	0%
11.	SEGURIDAD FÍSICA Y AMBIENTAL.	3	20%
12.	SEGURIDAD EN LA OPERATIVA.	4	29%
13.	SEGURIDAD EN LAS TELECOMUNICACIONES.	0	0%
14.	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	0	0%
15.	RELACIONES CON SUMINISTRADORES.	3	60%
16.	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	0	0%
17.	ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	1	25%
18.	CUMPLIMIENTO.	0	0%

Nota. La figura muestra una comparativa entre Implementación ISO/IEC 27002 vs Objetivos de Control

Figura 13

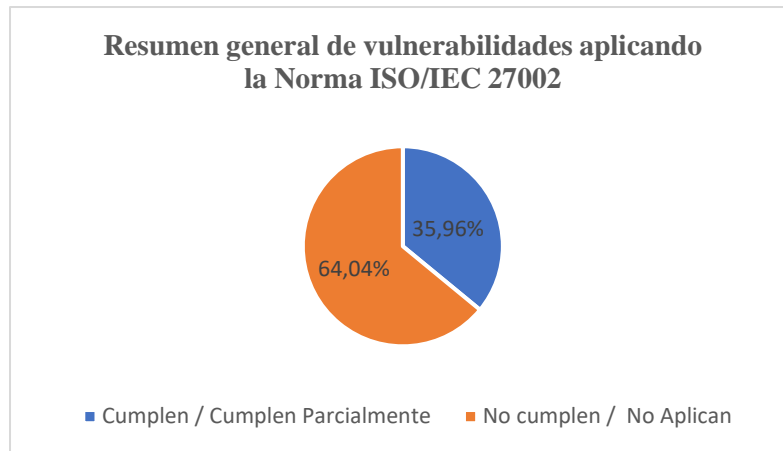
Resumen general de vulnerabilidades aplicando la norma ISO/IEC 27002

Resumen general de vulnerabilidades aplicando la norma ISO 27002		
ISO/IEC 27002:2013 Objetivos de Control		Total Criterios
5.	POLITICAS DE SEGURIDAD.	2
6.	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.	7
7.	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	6
8.	GESTIÓN DE ACTIVOS.	10
9.	CONTROL DE ACCESOS.	14
10.	CIFRADO.	2
11.	SEGURIDAD FÍSICA Y AMBIENTAL.	15
12.	SEGURIDAD EN LA OPERATIVA.	14
13.	SEGURIDAD EN LAS TELECOMUNICACIONES.	7
14.	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	13
15.	RELACIONES CON SUMINISTRADORES.	5
16.	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	7
17.	ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	4
18.	CUMPLIMIENTO.	8
TOTAL		114
PORCENTAJE		100%

Nota. En la tabla se muestra el resumen general de vulnerabilidades aplicando la norma ISO/IEC 27002.

Figura 14

Resultado del resumen de vulnerabilidades



Nota. En la figura se puede apreciar los resultados generales del resumen de vulnerabilidades.

Resultados: Se puede evidenciar en la Figura 13 y Figura 14, que la Facultad de Ingeniería en Sistemas Electrónica e Industrial perteneciente a la UTA, el cumplimiento con los criterios que establece la Norma ISO/IEC 27002, en cuestión del cumplimiento sobre la gestión de la seguridad de la información es tan solo del 35.96% frente al 64.04% de criterios no cumplidos.

Análisis: Como se observa en la Figura 12, se menciona que la Facultad de Ingeniería en Sistemas Electrónica e Industrial perteneciente a la UTA, cumple parcialmente con los controles de la norma ISO/IEC 27002. Por lo que para garantizar un adecuado funcionamiento en la institución se debe cumplir con las exigencias expuestas en la Norma Internacional.

Los resultado de la contribución de los controles mostrados en la Figura 15 , detallan la cantidad de controles y el nivel de cumplimiento con la norma, en la que permite llevar a cabo procedimientos de mejora.

Figura 15

Resultado de la contribución de los controles en base a la ISO/IEC 27002

Cantidad	Codigos Estado	Significado	Contribución %
12	D	El control se documentó e implementó	11%
13	MD	El Control se lleva a cabo y el proceso debe ser documentado para asegurar la repetibilidad del proceso y mitigar los riesgos.	11%
16	RD	El control no cumple las normas y debe ser rediseñado para cumplir con las normas	14%
51	PNP	El proceso no está en su lugar / no implementado. (Control requeridos ni documentado ni implementado)	45%
22	NA (No Aplicable)	El control no es aplicable para la empresa ni para el negocio	19%
114			

Nota. La figura muestra el resultado de los controles de la ISO/IEC 27002

Análisis de vulnerabilidades tecnológicas

Para cumplir con el análisis de vulnerabilidades, se tomó en consideración pruebas específicas que permitieron analizar el tráfico de la red mediante herramientas con software libre como se muestra a continuación:

A. Escaneo de puertos con la herramienta NMAP 7.94

Para el escaneo de puertos se utilizó la herramienta Nmap 7.94 en el Sistema Operativo Kali Linux versión 2023.3 amd64, instalado previamente sobre la máquina virtual Oracle VirtualBox versión 7.0.12. Esta herramienta permitió encontrar información de un determinado número de equipos encontrando puertos abiertos sobre determinados servicios, dando como resultado entrada libre a los atacantes informáticos.

Como se puede apreciar en la Figura 16, luego de realizar el escaneo de puertos en la red de la FISEI, se identifica que existen puertos abiertos asociados a los servicios tales como: ssh, http, ssh, ssl/http. Mysql, además se evidencia errores de compilación que corresponden a la conexión con los servicios anteriormente mencionados, esto usualmente puede generar conflictos con los nuevos servicios que la FISEI desee implementar en un futuro.

Figura 16

Servidor de aplicaciones FISEI GenDocs v2.0. con la dirección IP: 172.XX.XX.13.

```
(root@kali-redes)-[~]
# nmap -sS -sV 172. .13
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-18 19:05 -05
Nmap scan report for 172. .13
Host is up (0.00050s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh         OpenSSH 8.0 (protocol 2.0)
80/tcp    open  http        Apache httpd 2.4.37 ((AlmaLinux) OpenSSL/1.1.1k)
222/tcp   open  ssh         OpenSSH 8.0 (protocol 2.0)
443/tcp   open  ssl/http    Apache httpd 2.4.37 ((AlmaLinux) OpenSSL/1.1.1k)
3000/tcp  open  ppp?
3001/tcp  open  nessus?
3306/tcp  open  mysql       MySQL (unauthorized)
8080/tcp  open  http        (PHP 8.2.7)
3 services unrecognized despite returning data. If you know the service/version,
```

Nota. Resultado de aplicación del análisis de escaneo de puertos utilizando la Herramienta de análisis Nmap.

En cuanto a los equipos grabadores NVR de la FISEI cuenta con 2, a continuación, se muestra el escaneo respectivo de los equipos en la Figura 17 y Figura 18, ambos se someten a un análisis de puertos obteniendo como resultados los siguientes servicios abiertos que son: http, 80/tcp, ipcam, tcpwrapped, upnp, rtsp. Aparte se puede apreciar que tienen errores por no tener la versión actualizada del sistema Hikvision en el equipo, lo que ocasiona a los grabadores problemas de conectividad frecuentemente.

Figura 17

Cámara (Hikvision) NVR 1: 172.XX.XX.100

```
(root@kali-redes)-[~]
# nmap -sS -sV 172. .100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-18 19:01 -05
Nmap scan report for 172. .100
Host is up (0.00059s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Webs
8000/tcp  open  ipcam       Hikvision IPCam control port
10010/tcp open  tcpwrapped
49152/tcp open  upnp        Portable SDK for UPnP devices 1.6.18 (Linux 3.10.0_h
1 service unrecognized despite returning data. If you know the service/version,
SF-Port80-TCP:V=7.94%I=7%D=10/18%Time=653071EB%P=x86_64-pc-linux-gnu%r(Get
```

Nota. Resultado de la aplicación del análisis de escaneo de puertos utilizando la Herramienta de análisis Nmap, en el NVR 1 correspondiente al Bloque 2 de la FISEI.

Figura 18

Cámara (Hikvision) NVR 2: 172.XX.XX.200


```

(root@kali-redes)-[~]
# nmap -sS -sV 172.200
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-18 18:53 -05
Nmap scan report for 172.200
Host is up (0.00077s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Hikvision Network Video Recorder http admin
554/tcp   open  rtsp   Apple AirTunes rtspd
8000/tcp  open  ipcaml Hikvision IPCam control port
Service Info: OS: Mac OS X; Device: webcam; CPE: cpe:/o:apple:mac_os_x

Service detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 16.87 seconds

```

Nota. Resultado de la aplicación del análisis de escaneo de puertos utilizando la Herramienta de análisis Nmap, en el NVR 2 correspondiente al Bloque 1 de la FISEI.

En cuanto a la Figura 19, se observa una descripción de puertos y servicios abiertos correspondientes a los siguientes: http, msrpc, netbios-ssn, ssl/http, Microsoft-ds, enpp, mysql. Se identifica que la base de datos instalada en el equipo de prueba y desarrollo del sistema GenDocs v2.0. es MariaDB cuyo puerto es el 3306 que se encuentra abierto, todos estos servicios son de gran importancia y por lo que genera vulnerabilidades en el equipo antes mencionado.

Figura 19

Equipo de prueba y desarrollo del sistema GenDocs v2.0. con la dirección IP: 172.XX.XX.217

```

(root@kali-redes)-[~]
# nmap -sS -sV 172.217
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-18 19:20 -05
Nmap scan report for 172.217
Host is up (0.0011s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.56 ((Win64) OpenSSL/1.1.1t PHP/8.2.4)
135/tcp   open  msrpc   Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
443/tcp   open  ssl/http Apache httpd 2.4.56 (OpenSSL/1.1.1t PHP/8.2.4)
445/tcp   open  microsoft-ds?
2968/tcp  open  enpp?
3306/tcp  open  mysql   MariaDB (unauthorized)
MAC Address: C0:3F:D5:5E:AB:A2 (Elitegroup Computer Systems)
Service Info: Host: www.example.com; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 163.96 seconds

```

Nota. Resultado de la aplicación del análisis de escaneo de puertos utilizando la Herramienta de análisis Nmap.

En la Figura 20, se puede evidenciar el estado de los servicios abiertos tales como: http, msrpc, netbios-ssn, Microsoft-ds, enpp. Mediante la herramienta de análisis de puertos también se identificó el MAC Address. La información que maneja este departamento es de gran importancia para la FISEI, y según la fuente directa que utiliza el equipo del departamento antes mencionado se almacena información crucial para los procesos que deben cumplir los estudiantes de la FISEI para graduarse.

Figura 20

Equipo de Coordinación de la Unidad de Vinculación.: 172.XX.XX.212

```
(root@kali-redes)-[~]
# nmap -sS -sV 172. .212
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-10 15:59 -05
Nmap scan report for 172. .212
Host is up (0.0023s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
80/tcp    open  http             Microsoft IIS httpd 10.0
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
2968/tcp  open  enpp?
MAC Address: 4C:72:B9:24:CE:3C (Pegatron)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Nota. Equipo de Coordinación de la Unidad de Vinculación con la dirección IP: 172.XX.XX.212.

En la Figura 21, correspondiente al análisis de escaneo de puertos donde se evidencia los servicios: http, msrpc, netbios-ssn, Microsoft-ds, enpp. El departamento de la Unidad Académica de Titulación desempeña otras funciones paralelas como la Planificación y Evaluación Institucional. La información de ambas partes es almacenada en el equipo anteriormente mencionado sometido al análisis de puertos.

Figura 21

Equipo de la Unidad Académica de Titulación con la dirección IP: 172.XX.XX.55.

```
(root@kali-redes)-[~]
# nmap -sS -sV 172. .55
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-10 16:18 -05
Nmap scan report for 172. .55
Host is up (0.0021s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
80/tcp    open  http             Microsoft IIS httpd 10.0
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
7070/tcp  open  ssl/realserver?
MAC Address: C0:3F:D5:B8:35:04 (Elitegroup Computer Systems)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Nota. Resultado de la aplicación del análisis de escaneo de puertos utilizando la Herramienta de análisis Nmap.

Se puede evidenciar en la Figura 22, correspondiente al equipo de almacenamiento del departamento de programas de la Unidad de Titulación de Posgrado de la FISEI, tiene puertos abiertos correspondientes a los servicios: msrpc, netbios-ssn, Microsoft-ds, enpp, ms-wbt-server. Dicho departamento trabaja con gran cantidad de información sobre la cual cuentan con este equipo para alojar información relevante sobre los 5 últimos años acerca de los programas que se han ido dando en la FISEI.

Figura 22

Equipo de almacenamiento de programas de la Unidad de Titulación de Posgrado de la FISEI con la dirección IP: 172.XX.XX.123.

```

(root@kali-redes)-[~]
# nmap -sS -sV 172. .123
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-10 14:35 -05
Nmap scan report for 172. .123
Host is up (0.0034s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE      SERVICE      VERSION
135/tcp   open      msrpc        Microsoft Windows RPC
139/tcp   open      netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open      microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
2968/tcp  open      enpp?
3389/tcp  filtered  ms-wbt-server
49152/tcp open      msrpc        Microsoft Windows RPC
49153/tcp open      msrpc        Microsoft Windows RPC
49154/tcp open      msrpc        Microsoft Windows RPC
49155/tcp open      msrpc        Microsoft Windows RPC
49158/tcp open      msrpc        Microsoft Windows RPC
Service Info: Host: MAESTRIAS-04; OS: Windows; CPE: cpe:/o:microsoft:windows

```

Nota. Resultado de la aplicación del análisis de escaneo de puertos utilizando la Herramienta de análisis Nmap.

Mediante el análisis de escaneo de puertos mostrado en la Figura 23, correspondiente al personal administrativo encargado de realizar los respectivos procesos internos almacena información valiosa. El equipo mencionado tiene puertos abiertos que son: msrpc, netbios-ssn, Microsoft-ds, enpp, ms-wbt-server.

Figura 23

Equipo de la Unidad de Titulación de Posgrado de la FISEI.: 172.XX.XX.15

```

(root@kali-redes)-[~]
# nmap -sS -sV 172. .15
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-10 13:54 -05
Nmap scan report for 172. .15
Host is up (0.0046s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE      SERVICE      VERSION
135/tcp   open      msrpc        Microsoft Windows RPC
139/tcp   open      netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open      microsoft-ds?
2968/tcp  open      enpp?
3389/tcp  filtered  ms-wbt-server
7070/tcp  open      ssl/realserver?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

```

Nota. Resultado de la aplicación del análisis de escaneo de puertos utilizando la Herramienta de análisis Nmap.

Uno de los departamentos de gran importancia para la FISEI es el decanato, ya que es donde se tramita todos los procesos académicos relacionados con los distintos departamentos, dando la respectiva aprobación a los trámites pertinentes que se vayan solicitando. En la Figura 24, se puede evidenciar los puertos y servicios encontrados en el análisis de escaneo que son los siguientes: msrpc, netbios-ssn, microsoft-ds, enpp, ms-wbt-server.

Figura 24

Equipo de la Secretaria de Decanato de la FISEI con la dirección IP: 172.XX.XX.200.

```
(root@kali-redes)-[~]
# nmap -sS -sV 172. .200
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-10 13:15 -05
Nmap scan report for 172. .200
Host is up (0.0012s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE      SERVICE      VERSION
135/tcp   open      msrpc        Microsoft Windows RPC
139/tcp   open      netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open      microsoft-ds?
2968/tcp  open      enpp?
3389/tcp  filtered  ms-wbt-server
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Nota: Resultado de la aplicación del análisis de escaneo de puertos utilizando la Herramienta de análisis Nmap.

Uno de los departamentos de igual importancia para la FISEI es el Sub Decanato, ya que es donde igual tramita procesos academicos dando la respectiva aprobación a los trámites pertinentes que se vayan solicitando. En la Figura 25 se puede evidenciar los puertos y servicios encontrados en el análisis de escaneo que son los siguientes: msrpc, netbios-ssn, microsoft-ds, enpp, ms-wbt-server.

Figura 25

Equipo de la Secretaria de Sub Decanato de la FISEI.: 172.XX.XX.206

```
(root@kali-redes)-[~]
# nmap -sS -sV 172. .206
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-10 15:38 -05
Nmap scan report for 172. .206
Host is up (0.00064s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE      SERVICE      VERSION
135/tcp   open      msrpc        Microsoft Windows RPC
139/tcp   open      netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open      microsoft-ds?
3389/tcp  filtered  ms-wbt-server
7070/tcp  open      ssl/realserver?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Nota: Resultado de la aplicación del análisis de escaneo de puertos utilizando la Herramienta de análisis Nmap.

A continuación, en la Tabla 35 se aprecia un resumen de resultados de los escaneos realizados, correspondiente a los equipos con mayor grado de criticidad. Estos equipos informáticos albergan gran cantidad de información sumamente importante, así como los sistemas ejecutados por el personal administrativo. Se puede concluir que con ayuda de la herramienta NMAP se identificó puertos de servicios abiertos los mismos que generan vulnerabilidades en general a la FISEI.

Tabla 35

Listado general de puertos abiertos de los activos informáticos críticos de la FISEI.

PUERTO	PROTOCOLO	DESCRIPCIÓN	NÚMERO TOTAL DE EQUIPOS	ESTADO

22	TCP	ACCESO REMOTO A UN SERVIDOR SSH 8.0	1	ABIERTO
80	TCP	APACHE HTTPD 2.4.37, PHP/8.2.4	6	ABIERTO
443	TCP	APACHE HTTPD 2.4.37, OPEN SSL/1.1.1k	1	ABIERTO
443	TCP	APACHE HTTPD 2.4.56, OPEN SSL/1.1.1t PHP/8.2.4	2	ABIERTO
3000	TCP	SERVICIO PPP	1	ABIERTO
3001	TCP	NESSUS	1	ABIERTO
222	TCP	ACCESO REMOTO A UN SERVIDOR SSH 8.0	1	ABIERTO
3306	TCP	MYSQL MYSQL	2	ABIERTO
3389	TCP	FILETERED MS-WBT-SERVER	4	ABIERTO
8080	TCP	HTTP (PHP 8.2.7)	1	ABIERTO
8000	TCP	TCPWRAPPED	1	ABIERTO
49152	TCP	UPNP PORTABLE SDK FOR UPNP	1	ABIERTO
554	TCP	APPLE AIRTUNES RTSPD	1	ABIERTO
135	TCP	MSRPC MICROSOFT WINDOWS RPC	7	ABIERTO
2968	TCP	ENPP	5	ABIERTO
445	TCP	MICROSOFT-DS	7	ABIERTO
139	TCP	NETBIOS-SSN	7	ABIERTO
7070	TCP	SSL/REASERVER	3	ABIERTO

Nota: Esta tabla muestra un resumen de los puertos abiertos de los activos de información críticos de la FISEI.

B. Escaneo de puertos con la herramienta NESSUS

Con ayuda de la herramienta Nessus-10.6.1-ubuntu1404_amd64, instalada en el Sistema Operativo Kali Linux versión 2023.3 amd64. Nessus funciona mediante un navegador web que en su página oficial se debe proceder con el inicio de sesión, para realizar el análisis se

selecciona la opción Avanzado (Advanced Scan), se coloca el nombre del proceso, descripción, dirección IP para posteriormente guardar el escaneo y ejecutar el análisis de vulnerabilidades, y obtener un reporte en base CVSS v3.1 o sistema común de puntuación de vulnerabilidades, el mismo que es un estándar abierto, indica la gravedad que tiene una vulnerabilidad. Junto al reporte CVSS v3.1 también se puede identificar la calificación de prioridad de vulnerabilidad (VPR), mismo que arroja el resultado de priorizar la vulnerabilidad con mayor riesgo.

Se procedió con la detección de vulnerabilidades de los sistemas operativos de los activos informáticos críticos del listado detallado en la Tabla 35 pertenecientes a la FISEI, donde se encuentran almacenando gran cantidad de información. Esta herramienta permitió realizar un escaneo exhaustivo donde se puede evidenciar los niveles de riesgo que tiene ante posibles ataques informáticos. A continuación de muestra los resultados obtenidos de cada uno de los equipos:

1. Equipo: Servidor de aplicaciones FISEI GenDocs v2.0

Este equipo es de gran importancia para la FISEI ya que es donde se almacena la aplicación GenDocs v2.0 mismo que integra el proceso de graduados de los estudiantes que finalizaron la malla curricular, ingresando los trámites por secretaria de cada carrera, y luego por secretaria general que finaliza el proceso legal generando actas de los graduados. Para almacenar esta información lo hacen en una cuenta de Google Drive vinculada al aplicativo, el mismo debe ser protegido ya que esta información la tienen al alcance de cualquier persona que maneje el sistema y puede borrar dicha documentación por error o intencionalmente.

A continuación, se puede observar en la Figura 26, el reporte del análisis de vulnerabilidades encontradas en el Servidor de aplicaciones FISEI GenDocs v2.0., se muestran 46 resultados mismos que resaltan 1 crítico, 4 en medio, 2 en bajo y 39 en información; según el rango de puntuación VPR las vulnerabilidades con mayor índice de riesgo que se debe resolver corresponde a: 6.7 (PHP 8.2), 4.0 (HTTP TRACE), 6.5 (SSH Server CBC Mode Ciphers Enabled).

Figura 26

Servidor de aplicaciones FISEI GenDocs v2.0: 172.XX.XX.13

172. .13



Vulnerabilities Total: 46

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	6.7	179906	PHP 8.2.x < 8.2.9 Multiple Vulnerabilities
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	121479	web.config File Information Disclosure
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	6.5	70658	SSH Server CBC Mode Ciphers Enabled
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	18261	Apache Banner Linux Distribution Disclosure

Nota. Resultado de la aplicación del análisis de vulnerabilidades utilizando la Herramienta de análisis Nessus, al servidor de aplicaciones GenDocs v2.0 de la FISEI.

2. Equipo: Hikvision NVR 1.

El equipo Hikvision NVR 1, encargado almacenar las grabaciones de los respectivos ambientes de la FISEI correspondientes en gran mayoría al Bloque 2.

A continuación, se puede observar en la Figura 27, el reporte del análisis de vulnerabilidades encontradas en el equipo Hikvision NVR 1, se muestran 12 resultados 12 en información; las vulnerabilidades con riesgo que se debe resolver corresponden a: ICMP, HTTP Server Type and Version.

Figura 27

Equipo Hikvision NVR 1.

172. .100



Vulnerabilities Total: 12

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	54615	Device Type
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	10287	Traceroute Information

Nota: Resultado de la aplicación del análisis de vulnerabilidades utilizando la Herramienta de análisis Nessus, en el NVR 1 correspondiente al Bloque 2 de la FISEI.

3. Equipo: Hikvision NVR 2.

El equipo Hikvision NVR 2, encargado almacenar las grabaciones de los respectivos ambientes de la FISEI correspondientes en gran mayoría al Bloque 1.

A continuación, se puede observar en la, el reporte del análisis de vulnerabilidades encontradas en el equipo Hikvision NVR 1, se muestran 11 resultados, 11 en información; las vulnerabilidades con riesgo que se debe resolver corresponden a: ICMP, HTTP Server Type and Version.

Figura 28

172. 200



Vulnerabilities Total: 11

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	107057	Hikvision IP Camera Web Interface Detection
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	50350	OS Identification Failed
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	10287	Traceroute Information

Nota. Resultado de la aplicación del análisis de vulnerabilidades utilizando la Herramienta de análisis Nessus, en el NVR 2 correspondiente al Bloque 1 de la FISEI.

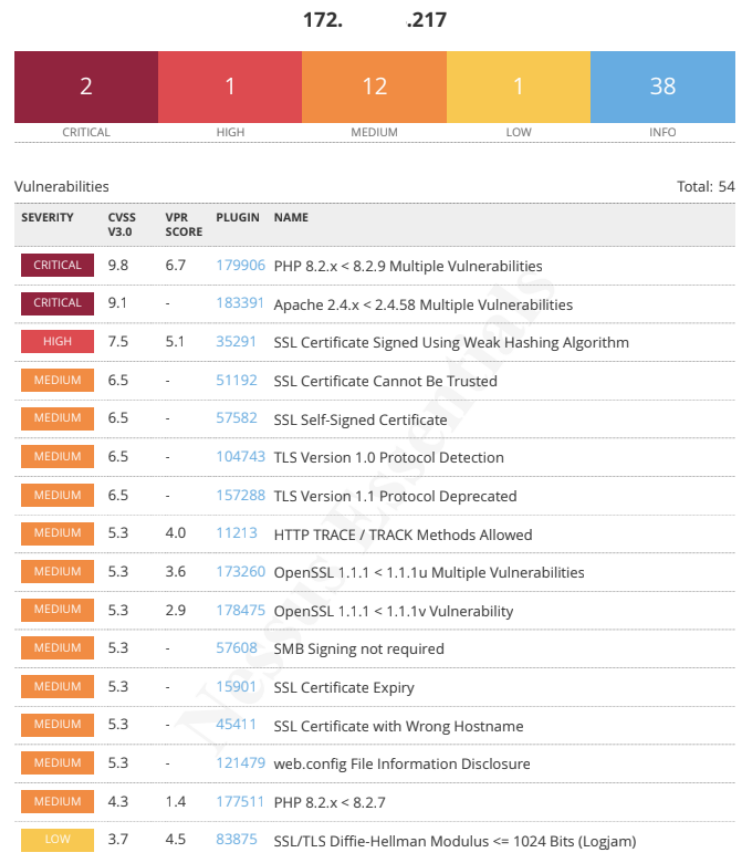
4. Equipo: Prueba y desarrollo del sistema GenDocs v2.0.

Este equipo es de gran importancia para la FISEI ya que es donde se realiza los cambios solicitados por parte del personal administrativo que ocupa el sistema GenDocs v2.0, el cual tiene toda la codificación del sistema y trabaja paralelamente con el servidor del aplicativo cuando ejecutan cambios y lo colocan en producción.

A continuación se puede observar en la Figura 29, el reporte del análisis de vulnerabilidades encontradas en el equipo de prueba y desarrollo del sistema GenDocs v2.0, se muestran 54 resultados mismos que resaltan 2 críticos, 1 alto, 12 en medio, 1 en bajo y 38 en información; según el rango de puntuación VPR las vulnerabilidades con mayor índice de riesgo que se debe resolver corresponde a: 6.7 (PHP 8.2), 5.1 (SSL), 4.0 (HTTP TRACE), 3.7 (SSH/TLS).

Figura 29

Equipo de prueba y desarrollo del sistema GenDocs v2.0.



Nota. Resultado del escaneo de vulnerabilidades utilizando la Herramienta de análisis Nessus.

5. Equipo: Coordinación de la Unidad de Vinculación

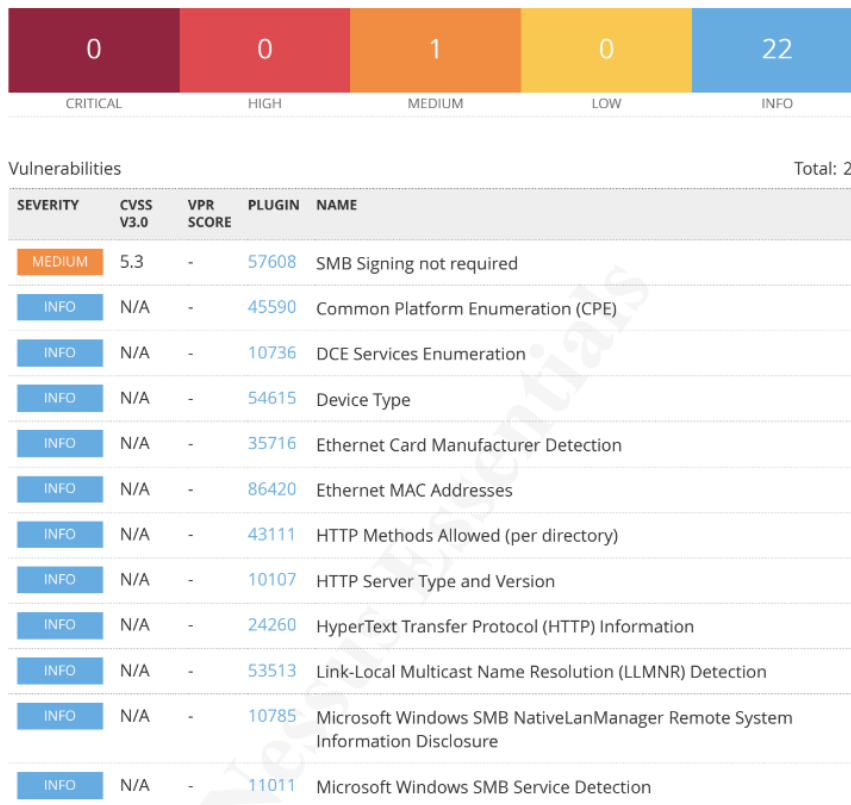
Este equipo es de gran importancia para la FISEI ya que es donde se almacena información sobre la coordinación con la vinculación con la sociedad en diferentes empresas, para que los estudiantes realicen sus prácticas profesionales mismo que representa un requisito crucial para que puedan graduarse.

A continuación, se puede observar en la Figura 30, el reporte del análisis de vulnerabilidades encontradas en el equipo de Coordinación de la Unidad de Vinculación, se muestran 23 resultados mismos que resalta 1 en medio, y 22 en información; las vulnerabilidades con riesgo que se debe resolver corresponden a: 5.3 (SMB Signing not required), HTTP Server Type and Version, (DCE Services Enumeration).

Figura 30

Equipo de Coordinación de la Unidad de Vinculación

172. .212



Nota: Resultado del escaneo de vulnerabilidades utilizando la Herramienta de análisis Nessus.

6. Equipo: Unidad Académica de Titulación FISEI

Este equipo es de gran importancia para la FISEI ya que es donde se almacena y gestiona información crucial sobre la Unidad Académica de Titulación cuyas funciones son recibir, analizar y gestionar la documentación relacionada con el proceso de titulación de acuerdo con lo establecido en el reglamento institucional.

A continuación, se puede observar en la Figura 31, el reporte del análisis de vulnerabilidades encontradas en el equipo de la Unidad Académica de Titulación FISEI, se muestran 37 resultados mismos que resalta 4 en medio, y 33 en información; las vulnerabilidades con riesgo que se debe resolver corresponden a: 6.5 (SSL Certificate Cannot Be Trusted), Common Platform Enumeration CPE, HTTP Server Type and Version, (DCE Services Enumeration).

Figura 31

Unidad Académica de Titulación FISEI

172. .55



Vulnerabilities Total: 37

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	5.3	-	57608	SMB Signing not required
MEDIUM	5.3	-	45411	SSL Certificate with Wrong Hostname
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10736	DCE Services Enumeration
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	53513	Link-Local Multicast Name Resolution (LLMNR) Detection

Nota: Resultado del escaneo de vulnerabilidades utilizando la Herramienta de análisis Nessus.

7. Equipo de almacenamiento de programas de la Unidad de Titulación de Posgrado

Este equipo es de gran importancia para la FISEI ya que es donde se almacena información sobre la Unidad Académica de Posgrado cuyas funciones es documentar los procesos de titulación de los estudiantes, así como los programas de maestría que se van presentando de acuerdo con lo establecido en el reglamento institucional.

A continuación, se puede observar en la, el reporte del análisis de vulnerabilidades encontradas en el equipo de la Unidad de Titulación de Posgrado FISEI, se muestran 23 resultados mismos que resalta 1 crítico, 1 en medio, y 21 en información; según el rango de puntuación VPR las vulnerabilidades con mayor índice de riesgo que se debe resolver corresponde a: 10.0 (Unsupported Windows OS remote), 5.3 (SMB Signing not required), (DCE Services Enumeration).

Figura 32

Unidad de Titulación de Posgrado

172. .123



Vulnerabilities Total: 23

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	10.0	-	108797	Unsupported Windows OS (remote)
MEDIUM	5.3	-	57608	SMB Signing not required
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10736	DCE Services Enumeration
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry

Nota. Resultado del escaneo de vulnerabilidades utilizando la Herramienta de análisis Nessus.

8. Equipo de secretaria de programas de la Unidad de Titulación de Posgrado

Este equipo es de gran importancia para la FISEI ya que es donde se gestiona la información sobre la Unidad Académica de Posgrado cuyas funciones es gestionar los procesos de titulación de los estudiantes, así como los programas de maestría que se van presentando de acuerdo con lo establecido en el reglamento institucional.

A continuación se puede observar en la Figura 33, el reporte del análisis de vulnerabilidades encontradas en el equipo de la secretaria de la Unidad de Titulación de Posgrado FISEI, se muestran 29 resultados mismos que resalta 4 en medio, y 29 en información; según el rango de puntuación VPR las vulnerabilidades con mayor índice de riesgo que se debe resolver corresponden a: 6.5 (SSL Certificate Cannot Be Trusted), 5.3 (SMB Signing not required), (DCE Services Enumeration).

Figura 33

Secretaria de programas de la Unidad de Titulación de Posgrado

172. .15



Vulnerabilities Total: 33

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	5.3	-	57608	SMB Signing not required
MEDIUM	5.3	-	45411	SSL Certificate with Wrong Hostname
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10736	DCE Services Enumeration
INFO	N/A	-	54615	Device Type
INFO	N/A	-	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection

Nota. Resultado del escaneo de vulnerabilidades utilizando la Herramienta de análisis Nessus.

9. Equipo de secretaria de Información de la FISEI

Este equipo es de gran importancia para la FISEI ya que es donde se gestiona y almacena información sobre la secretaria de Información cuyas funciones son el ingreso de todos los trámites y procesos de la FISEI que se van presentando de acuerdo con lo establecido en el reglamento institucional.

A continuación se puede observar en la Figura 34, el reporte del análisis de vulnerabilidades encontradas en el equipo de la secretaria de Información de la FISEI, se muestran 23 resultados mismos que resalta 1 crítico, 1 en medio, y 21 en información; según el rango de puntuación VPR las vulnerabilidades con mayor índice de riesgo que se debe resolver corresponden a: 10.0 (Unsupported Windows OS remote), 5.3 (SMB Signing not required), (DCE Services Enumeration).

Figura 34

Secretaria de Información de la FISEI

172. .203



Vulnerabilities

Total: 23

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	10.0	-	108797	Unsupported Windows OS (remote)
MEDIUM	5.3	-	57608	SMB Signing not required
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10736	DCE Services Enumeration
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection

Nota. Resultado del escaneo de vulnerabilidades utilizando la Herramienta de análisis Nessus.

10. Equipo de secretaria de Decanato

Este equipo es de gran importancia para la FISEI ya que es donde se gestiona y almacena información sobre la secretaria de decanato cuyas funciones son tramitar, aprobar, designar los procesos que se van presentando de acuerdo con lo establecido en el reglamento institucional.

A continuación, se puede observar en la Figura 35, el reporte del análisis de vulnerabilidades encontradas en el equipo de la secretaria de decanato de la FISEI, se muestran 18 resultados mismos que resalta 1 en medio, y 17 en información; según el rango de puntuación CVSS las vulnerabilidades con mayor índice de riesgo que se debe resolver corresponden a: 5.3 (SMB Signing not required), ICMP (Timestamp Request Remote Date Disclosure), (DCE Services Enumeration).

Figura 35

Secretaria de decanato

172. 6.200



Vulnerabilities Total: 18

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	5.3	-	57608	SMB Signing not required
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10736	DCE Services Enumeration
INFO	N/A	-	54615	Device Type
INFO	N/A	-	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

Nota. Resultado del escaneo de vulnerabilidades utilizando la Herramienta de análisis Nessus.

11. Equipo de secretaria de Sub-Decanato

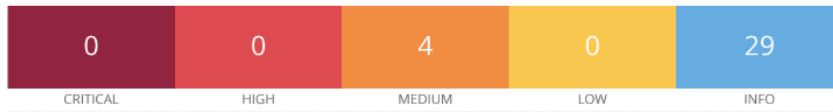
Este equipo es de gran importancia para la FISEI ya que es donde al igual que Decanato se gestiona y almacena información sobre la secretaria de sub-decanato cuyas funciones son tramitar, aprobar, designar los procesos que se van presentando de acuerdo con lo establecido en el reglamento institucional.

A continuación, se puede observar en la Figura 36, el reporte del análisis de vulnerabilidades encontradas en el equipo de la secretaria de sub-decanato de la FISEI, se muestran 33 resultados mismos que resalta 4 en medio, y 29 en información; según el rango de puntuación CVSS las vulnerabilidades con mayor índice de riesgo que se debe resolver corresponden a: 6.5 (SSL Certificate Cannot Be Trusted), 5.3 (SMB Signing not required), 5.3 (SSL Certificate with Wrong Hostname), ICMP (Timestamp Request Remote Date Disclosure), (DCE Services Enumeration), (DCE Services Enumeration).

Figura 36

Secretaria de Sub-Decanato

172. .206



Vulnerabilities

Total: 33

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	5.3	-	57608	SMB Signing not required
MEDIUM	5.3	-	45411	SSL Certificate with Wrong Hostname
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10736	DCE Services Enumeration
INFO	N/A	-	54615	Device Type
INFO	N/A	-	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection






Nota. Resultado del escaneo de vulnerabilidades utilizando la Herramienta de análisis Nessus.

A continuación, en la Tabla 36, se muestra un resumen de los resultados del análisis de vulnerabilidades de los equipos correspondiente al listado de activos informáticos críticos de la FISEI, se menciona que al obtener varios reportes con gran cantidad de información, se optó por presentar los demás resultados en el apartado de los Anexos II del presente proyecto de tesis, en la que se puede evidenciar de manera detallada cada resultado obtenido de los activos críticos anteriormente mencionados.

Tabla 36

Resumen de los resultados del análisis de vulnerabilidades utilizando la Herramienta Nessus

Dirección IP	Nombre	Resultado del Análisis de Vulnerabilidades										
172.XX.XX.13	Servidor de aplicaciones FISEI GenDocs v2.0.	<table border="1"> <tr> <td>1</td> <td>0</td> <td>4</td> <td>2</td> <td>39</td> </tr> <tr> <td>CRITICAL</td> <td>HIGH</td> <td>MEDIUM</td> <td>LOW</td> <td>INFO</td> </tr> </table>	1	0	4	2	39	CRITICAL	HIGH	MEDIUM	LOW	INFO
1	0	4	2	39								
CRITICAL	HIGH	MEDIUM	LOW	INFO								
172.X.X.100	Cámaras de la FISEI	<table border="1"> <tr> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>12</td> </tr> <tr> <td>CRITICAL</td> <td>HIGH</td> <td>MEDIUM</td> <td>LOW</td> <td>INFO</td> </tr> </table>	0	0	0	0	12	CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	12								
CRITICAL	HIGH	MEDIUM	LOW	INFO								
172.XX.XX.20 0	Cámaras de la FISEI	<table border="1"> <tr> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>11</td> </tr> <tr> <td>CRITICAL</td> <td>HIGH</td> <td>MEDIUM</td> <td>LOW</td> <td>INFO</td> </tr> </table>	0	0	0	0	11	CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	11								
CRITICAL	HIGH	MEDIUM	LOW	INFO								
172.X.X.217	Administración de Redes.	<table border="1"> <tr> <td>2</td> <td>1</td> <td>12</td> <td>1</td> <td>38</td> </tr> <tr> <td>CRITICAL</td> <td>HIGH</td> <td>MEDIUM</td> <td>LOW</td> <td>INFO</td> </tr> </table>	2	1	12	1	38	CRITICAL	HIGH	MEDIUM	LOW	INFO
2	1	12	1	38								
CRITICAL	HIGH	MEDIUM	LOW	INFO								
172.X.X.212	Coordinación de la Unidad de Vinculación FISEI.	<table border="1"> <tr> <td>0</td> <td>0</td> <td>1</td> <td>0</td> <td>22</td> </tr> <tr> <td>CRITICAL</td> <td>HIGH</td> <td>MEDIUM</td> <td>LOW</td> <td>INFO</td> </tr> </table>	0	0	1	0	22	CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	1	0	22								
CRITICAL	HIGH	MEDIUM	LOW	INFO								
172.XX.XX.55	Unidad Académica de Titulación.	<table border="1"> <tr> <td>0</td> <td>0</td> <td>4</td> <td>0</td> <td>33</td> </tr> <tr> <td>CRITICAL</td> <td>HIGH</td> <td>MEDIUM</td> <td>LOW</td> <td>INFO</td> </tr> </table>	0	0	4	0	33	CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	4	0	33								
CRITICAL	HIGH	MEDIUM	LOW	INFO								
172.X.X.123	Equipo de almacenamiento de programas											

	de la Unidad de Titulación de Posgrado de la FISEI	
172.XX.XX.15	Unidad de Titulación de Posgrado de la FISEI.	
172.XX.X.203	Secretaria de Información – FISEI.	
172.X.X6.200	Secretaria de Decanato.	
172.X.X.206	Secretaria Sub Decanato	
Resultados generales finales		5 1 32 3 272

Nota: Esta tabla muestra un resumen de los resultados del análisis de vulnerabilidades utilizando la Herramienta Nessus.

Interpretación de resultados del escaneo realizado anteriormente con le herramienta Nessus se encontró lo siguiente:

1. En los equipos se aprecia vulnerabilidades sobre SSL (Secure Sockets Layer) con relación a la firma de certificaciones, esto es importante considerar ya que un atacante puede generar otro certificado con las mismas características, dando la posibilidad que el atacante suplante la identidad y se haga pasar por el servicio afectado.
2. En el servidor se puede detectar como Base de Datos al servicio MySQL Server permitiendo registros de servicios desde un host remoto, esto ocasiona que cualquier atacante pueda detectar este problema y apoderarse de los datos.
3. Se puede identificar que el servicio SSH se encuentra habilitado y cualquier conexión entrante que utilice libssh tiene un gran riesgo de accesos no autorizados.

4. Se detecta el uso de PHP 8.2, siendo uno de los lenguajes menos seguros, y para ejecutar el software en internet se debe conectar con un hosting lo que lo hace más vulnerable.
5. Se aprecia el uso del protocolo ICMP, entre sus inconvenientes de su uso es que necesita estar con privilegios de root para su ejecución dado a que utiliza sockets RAW.
6. El uso de Apache 2.4 es detectado como vulnerabilidad crítica, dado a que cualquier atacante externo podría llegar a leer cualquier archivo, esto es posible cuando hacen uso de un path transversal que les permita mapear URLs.
7. En cuanto al protocolo TLS se ha identificado que está desactualizado lo que genera brechas de seguridad.

FASE 2: MODELO DE GESTIÓN DE SEGURIDAD DE ACUERDO A LAS BUENAS PRÁCTICAS ESTABLECIDAS POR LA NORMA ISO/IEC 27002

A continuación, se presenta el modelo de Gestión de la Seguridad de la Información mismo que fue desarrollado bajo algunos criterios entre los principales destacan una identificación de activos críticos, evaluación y análisis de riesgos informático, aplicable en el departamento de Administración de Redes de la Facultad de Ingeniería en Sistemas Electrónica e Industrial de la UTA, mismo que se encuentra ubicado en el Campus Huachi, del cantón Ambato.

Se debe considerar que las políticas presentadas en este Modelo de Gestión de la Seguridad de la Información son una propuesta de mejora que deberá ser autorizada por la máxima autoridad de la institución, para su desarrollo a la fase de implementación, mismo que va dirigido a todo el personal que labora en la FISEI, y de manera específica al personal del departamento de Administración de Redes.

6. Aspectos organizativos de la seguridad de la información.

6.1 Organización interna.

1. Nombrar un alto ejecutivo dedicado a supervisar el cumplimiento y la implementación de políticas y procedimientos de seguridad de la información.
2. Ejecutar auditorías internas dentro del departamento de Administración de redes de la FISEI.

3. Establecer programas de concientización y capacitación en seguridad de la información dentro de la FISEI, al menos cada 6 meses para garantizar que todo el personal comprendan sus responsabilidades en las mejores prácticas de seguridad.
4. El contacto con las autoridades debe ser abierto y transparente, en todas las interacciones que la comunidad universitaria crea necesario que se proporcione autorización o información.
5. El personal de la FISEI debe notificar de manera inmediata en el caso de existir sospechas o incidentes relacionados a la seguridad de la información.
6. El encargado de administrar los sistemas de información de la FISEI, con la debida autorización de la máxima autoridad de la facultad, concede los permisos de acceso fundados en la necesidad del usuario y los roles asignados al proyecto o sistema que desempeñara en su trabajo.
7. Se prohíbe el acceso físico, a personal no autorizado a las áreas de trabajo donde se encuentren los sistemas informáticos críticos.
8. Realizar copias de seguridad periódicas, al menos 1 vez a la semana de los datos ingresados y generados tanto de la Base de Datos como de los reportes finales del sistema GenDocs que se almacenan en el Google Drive automáticamente, alojándolos en otro sistema de almacenamiento como puede ser Microsoft OneDrive, Dropbox, etc.
9. En caso de ocurrir alguna falla con el sistema GenDocs, con autorización del jefe del área de Administración de Redes, restaurar inmediatamente la información con los últimos respaldos.

6.2 Dispositivos para movilidad y teletrabajo.

1. En el caso del uso de contraseñas es responsabilidad de la comunidad universitaria establecer contraseñas seguras, que garantice la protección contra el acceso no autorizado.

2. Como departamento de Administración de Redes responsable de asegurar la información, debe socializar a la comunidad universitaria la asignación de contraseñas seguras y complejas asociadas a sus respectivas cuentas, así como cambiarlas periódicamente.

3. El acceso remoto a la red de la facultad y por ende a la universidad, solo es permitido a aquel personal autorizado tanto por su supervisor y el departamento de Talento Humano de la UTA, para trabajar mediante teletrabajo.

4. El departamento de Administración de Redes luego de una previa autorización de la DITIC, es el responsable de permitir el acceso a una conexión segura mediante VPN (Red Privada Virtual), a través de la instalación y configuración del programa FortiClient en los equipos del personal universitario.

5. Todo el personal administrativo y docentes que se acojan al servicio de teletrabajo es responsable de proteger la confidencialidad, tanto la configuración del programa FortiClient, como del uso que se dé a la plataforma de documentación Quipux de la universidad.

6. Como facultad responsable buscará gestionar capacitaciones continuas sobre las buenas prácticas para el teletrabajo, mediante el cumplimiento disciplinario del cumplimiento de las directrices establecidas por la FISEI.

7. El incumplimiento de las políticas informáticas puede resultar en acciones disciplinarias, incluyendo la revocación del acceso remoto.

9. Control de Accesos.

Las políticas de control de acceso son fundamentales para garantizar la seguridad de la información y proteger los recursos tecnológicos de una institución. A continuación, se detallan algunas de las principales políticas que suelen incluirse.

9.1 Requisitos de negocio para el control de accesos.

1. El departamento de Administración de Redes es el responsable de la identificación y clasificación de los tipos de información sensible y crítica que maneja la facultad.
2. El acceso a la información sensible requerirá una autorización de los supervisores de cada departamento de la facultad.
3. Como facultad responsable proporcionará capacitación regular al personal, sobre la importancia de la restricción de acceso a sus respectivos sistemas y equipos informáticos, asociándolos a las mejores prácticas para su seguridad.
4. El departamento de Administración de Redes tiene la responsabilidad de llevar a cabo auditorías periódicas al menos cada 6 meses para evaluar el cumplimiento de las restricciones de acceso.

9.2 Gestión de acceso de usuario.

1. Los sistemas informáticos desarrollados internamente dentro de la FISEI, deben ser asociados a un ID único correspondiente a las credenciales de cada personal vinculado a su respectivo rol que desempeña en la facultad.
2. Los accesos a los diferentes sistemas de la facultad son otorgados por el departamento de Administración de Redes, correspondiente a las funciones y responsabilidades del personal a cargo, y se revocarán inmediatamente en el caso de finalizar su contrato o desvinculación de la FISEI.
3. El departamento de Administración de Redes mantendrá registros detallados de los accesos, incluyendo la identidad del usuario, fecha, hora y acciones realizadas en los sistemas.
4. El departamento de Administración de Redes realizará revisiones regulares de los registros de acceso para garantizar el cumplimiento de las políticas.
5. Por el incumplimiento de estas políticas puede resultar en medidas disciplinarias, incluyendo la desvinculación definitiva del personal.

9.3 Responsabilidades del usuario.

1. Los usuarios son responsables de mantener en secreto sus credenciales de acceso a los respectivos sistemas y no compartirlas con otros individuos.
2. El personal asociado a los sistemas informáticos de la FISEI, deberá notificar inmediatamente cualquier sospecha de compromiso de sus credenciales o pérdida de las mismas al personal encargado de los sistemas informáticos.
3. El personal del departamento de Administración de Redes debe proteger la información confidencial y no divulgarla a personas no autorizadas o ajenas a la misma.
4. El departamento de Administración de Redes debe mantener actualizado el software y firmware de sus dispositivos para mitigar vulnerabilidades de seguridad.

9.4 Control de acceso a sistemas y aplicaciones.

1. Con relación a los privilegios de acceso, el departamento de Administración de Redes acorde con las funciones de cada uno del personal permitirá el acceso al mínimo necesario para cumplir con sus tareas asignadas según su rol asignado previamente.
2. El departamento de Administración de Redes mantendrá métodos seguros de autenticación, como contraseñas fuertes que convine mayúsculas, minúsculas, caracteres especiales.
3. El departamento de Administración de Redes debe implementar medidas de seguridad física para proteger el acceso a instalaciones y equipos informáticos críticos de la facultad.

Esta Política de Restricción de Acceso a la Información es obligatoria y debe ser seguida estrictamente por todo el personal para garantizar la seguridad y confidencialidad de la información de la FISEI.

11. Seguridad Física y Ambiental

Una sólida política informática de seguridad física y ambiental es esencial para salvaguardar los activos digitales y la integridad de la información de una FISEI. A continuación, se detallan algunos puntos clave:

11.1 Áreas seguras.

1. El acceso a las áreas críticas de la FISEI estará restringido únicamente al personal autorizado que necesite acceso para cumplir con sus responsabilidades asignadas.
2. El departamento de Administración de Redes llevará un registro y supervisar el acceso a las áreas seguras, garantizando la detección temprana de posibles incidentes.
3. Instalar cerraduras de seguridad y sistemas de control de acceso para garantizar que solo personal autorizado pueda ingresar a las áreas seguras.
4. Implementar y monitorizarlos métodos de extinción de incendios y protocolos para minimizar el riesgo de daño por fuego en las áreas seguras.
5. Mantener condiciones ambientales adecuadas que incluyan un control de temperatura y humedad, donde se pueda garantizar el correcto funcionamiento de los equipos informáticos.
6. Se instalarán sistemas de UPS para proporcionar energía de respaldo y garantizar la continuidad de operaciones en caso de cortes de energía.
7. Todo incidente o actividad sospechosa en las áreas seguras deberá ser informado inmediatamente a los responsables del departamento de Administración de Redes de la FISEI.

11.2 Seguridad de los equipos.

1. El mantenimiento de los equipos informáticos debe estar a cargo del personal autorizado del departamento de Administración de Redes, y se debe realizar de forma periódica cada 6 meses.

2. El departamento de Administración de Redes deberá configurar el bloqueo de pantalla que es fundamental para prevenir el acceso no autorizado a la información confidencial de la FISEI.

3. El personal responsable de respaldar cualquier dato necesario antes de la eliminación de datos en sus dispositivos de almacenamiento deberá notificar al departamento de Administración de Redes.

4. Todo el personal universitario perteneciente a la FISEI debe recibir capacitación sobre los procedimientos adecuados para el retiro y la reutilización de dispositivos de almacenamiento, así como sobre la importancia de la eliminación segura de datos.

12. Seguridad en la Operativa

12.1 Responsabilidades y procedimientos de operación.

1. El personal universitario perteneciente a la FISEI (usuario), es responsable de utilizar los recursos informáticos de manera ética y profesional, demostrándose así un correcto uso de software y hardware.

2. Cada usuario tiene como responsabilidad de proteger la confidencialidad e integridad de la información.

3. Los usuarios deben informar cualquier incidente de seguridad o irregularidad en el funcionamiento de los diferentes sistemas de inmediato al departamento de Administración de Redes de la FISEI.

4. Al finalizar la relación laboral, los usuarios deben seguir los procedimientos de salida establecidos por la UTA, así como de la FISEI, incluyendo la devolución de dispositivos a su cargo y la revocación de accesos a los sistemas dejando un informe de avance hasta el último día de labores cumplidas.

12.2 Protección contra código malicioso.

1. El departamento de Administración de Redes debe llevar un control estricto de la instalación de antivirus en todos los equipos del personal universitario perteneciente a la FISEI (usuario).
2. Los usuarios son responsables de mantener informado al departamento de Administración de Redes, en caso de existir alguna actualización en los sistemas operativos que requiera confirmación por parte del administrador, como es el caso de sistemas operativos, antivirus y otras aplicaciones instaladas en cada equipo respectivamente.
3. Los usuarios deben participar activamente en programas de formación que la FISEI organice en temas de seguridad de la información para capacitarse sobre las amenazas de seguridad y cómo reconocer posibles riesgos.
4. El departamento de Administración de Redes llevará a cabo un procedimiento de respuesta a incidentes para actuar de manera rápida y eficaz en caso de una infección por código malicioso.

12.3 Copias de seguridad.

1. El personal universitario perteneciente a la FISEI (usuario), son responsables de clasificar la información crítica que vaya generando para su respaldo respectivo, si es el caso solicitar al departamento de Administración de Redes se haga una copia de seguridad en otro sitio a parte.
2. El departamento de Administración de Redes en coordinación con los usuarios de cada departamento de la FISEI, realizará copias de seguridad de ser el caso sobre información crítica, asociados a la frecuencia de cambio de datos.
3. Toda plataforma o sistemas que maneje información crítica deben incluirse en los procesos de copias de seguridad.

4. Las respectivas autoridades de la FISEI en conjunto con el departamento de Administración de redes deben coordinar los métodos adecuados para realizar copias de seguridad, ya sean almacenados en medios seguros tanto dentro como fuera de la institución como es el almacenamiento en la nube.
5. Las copias de seguridad almacenadas fuera de la FISEI deben estar encriptadas para garantizar la confidencialidad de la información.
6. Las claves de encriptación se manejarán de manera segura y solo estarán disponibles para personal autorizado del departamento de Administración de Redes.
7. El departamento de Administración de redes realizará pruebas periódicas de restauración para verificar la integridad y la eficacia de las copias de seguridad.
8. Las pruebas de restauración de la información deben incluir la recuperación de datos críticos y la validación de la continuidad del servicio y operaciones en la FISEI.
9. El departamento de Administración de redes tendrá designado al personal responsable de la planificación, ejecución y supervisión de las copias de seguridad.

12.4 Registro de actividad y supervisión.

1. El departamento de Administración de Redes llevará un registro de actividad y supervisión documentado, de todos los sistemas y aplicaciones críticas.
2. Dichos registros deben capturar eventualidades relevantes, como accesos, modificaciones de configuración, intentos de acceso no autorizado y otros eventos importantes.
3. El acceso a los registros de actividad estará restringido solo al personal autorizado.

4. El departamento de Administración de Redes, garantizará la privacidad y confidencialidad de la información sensible contenida en los registros.
5. El personal encargado recibirá capacitación periódica sobre la importancia de los registros de actividad y la supervisión para la seguridad de la información.

12.5 Control del software en explotación.

1. Todo software utilizado en la FISEI debe contar con licencias válidas y cumplir con los términos y condiciones establecidos por cada proveedor.
2. El uso de software sin licencia o pirata está estrictamente prohibido en la FISEI.
3. El personal universitario perteneciente a la FISEI (usuario), y administradores de sistemas deben asegurarse de que todo software en explotación se mantenga actualizado con las últimas versiones y parches de seguridad.
4. La instalación de software en los sistemas de la FISEI solo podrá ser realizada por personal autorizado del departamento de Administración de Redes.
5. Los usuarios no deben descargar ni ejecutar software sin la aprobación del departamento de Administración de Redes.
6. El usuario es responsable de no hacer clic en enlaces ni descargar archivos de fuentes no verificadas, en el caso de existir alguna duda sobre la procedencia de un mensaje de una fuente desconocida, se deberá informar inmediatamente al departamento de Administración de Redes.
7. La descarga de archivos ejecutables o de dudosa procedencia estará prohibida en los equipos informáticos de la FISEI.

12.6 Gestión de la vulnerabilidad técnica.

1. El departamento de Administración de Redes debe mantener un inventario actualizado de todos los activos de hardware y software utilizados en la FISEI.
2. Identificar y clasificar la importancia de los activos críticos para el funcionamiento de la FISEI.
3. Se debe realizar evaluaciones regulares de vulnerabilidades en sistemas, aplicaciones y redes utilizando herramientas y técnicas actualizadas por parte del departamento de Administración de Redes.
4. Priorizar las vulnerabilidades identificadas acorde a su gravedad y riesgo potencial.
5. El departamento de Administración de Redes tendrá una configuración segura que limite la instalación no autorizada de software y refuercen los sistemas informáticos.
6. El departamento de Administración de Redes debe documentar los procedimientos y decisiones relacionados con la gestión de vulnerabilidades.

12.7 Consideraciones de las auditorías de los sistemas de información.

1. El departamento de Administración de Redes establecerá ciclos regulares de auditorías para cubrir la seguridad de los componentes críticos del entorno de tecnología de la información.
2. Con la autorización de los directivos de la FISEI debe establecer un programa anual de auditorías basado en la criticidad de los sistemas y procesos que se manejen.
3. El departamento de Administración de Redes mantendrá una documentación detallada de los procedimientos de auditoría, hallazgos y recomendaciones, para una mejora continua.
4. La información obtenida durante las auditorías se considerará confidencial y se compartirá únicamente con personas autorizadas.

5. El departamento de Administración de Redes realizará un informe de carácter formal de auditoría, donde se incluirá hallazgos, recomendaciones y su respectivo plan de acción para abordar las áreas de mejora identificadas.

6. Como responsabilidad de la gestión de la FISEI proporcionará capacitación regular al personal universitario perteneciente a la FISEI (usuario), para aumentar la conciencia sobre la importancia de las auditorías y su papel en la mejora continua de la seguridad de la información.

16 Gestión de Incidentes de Seguridad de la Información

16.1. Gestión de incidentes de seguridad de la información y mejoras.

1. La máxima autoridad de la FISEI, debe designar un Equipo de Respuesta a Incidentes (ERT) con sus roles y responsabilidades claramente establecidos.

2. En caso de ocurrir algún tipo de incidente de seguridad de la información notificar de manera inmediata al departamento de Administración de Redes específicamente al equipo ERT.

3. El departamento de Administración de redes, desarrollara de manera continua un proceso de clasificación para evaluar la gravedad y la urgencia de los incidentes que pueden ocurrir en la FISEI.

4. La FISEI debe fomentar la capacitación continua al personal sobre las últimas amenazas de seguridad y mejores prácticas que generen conciencia sobre la importancia de la seguridad informática.

5. El departamento de Administración de Redes debe establecer una sólida base para gestionar incidentes de seguridad y mejorar continuamente su postura el tema de vulnerabilidades de la información.

FASE 3: VERIFICACIÓN DEL MODELO DE GESTIÓN DE SEGURIDAD DE ACUERDO A LAS BUENAS PRÁCTICAS ESTABLECIDAS POR LA NORMA ISO/IEC 27002

Verificar el cumplimiento de las Políticas de seguridad de la información de acuerdo a las tablas propuestas en el desarrollo del proyecto, en apartado de verificación correspondientes a las Tabla 37 hasta la Tabla 48, mismas que son una propuesta de verificación y pueden ser utilizadas a convenir.

Para realizar una correcta verificación en cuanto a las buenas prácticas de la norma ISO/IEC 27002 y garantizar de esa manera el cumplimiento de la misma se presenta los siguientes formatos que ayudarán a tener un mejor control.

En la Tabla 37, se hace referencia a un procedimiento de seguimiento y verificación del CONTROL 10, correspondiente al cifrado, en el cual se debe garantizar el uso de controles criptográficos, por ello se presenta un modelo de matriz el cual puede ser tomado como referencia para una futura implementación.

Tabla 37

Registro de uso de encriptación de información

REGISTRO DE USO DE NECESIDAD DE ENCRYPTACIÓN DE INFORMACIÓN					
Responsable:			Fecha:		
Nombre del departamento:					
Código del equipo:		Equipo perteneciente a:			
Nº	Dirección de la unidad de almacenamiento	Necesita encriptación		Tipo de encriptación utilizada	Herramienta Utilizada
		SI	NO		

Nota. En la tabla se muestra un conjunto de requerimientos básicos para un registro de encriptación de información, asociados a la Norma ISO/IEC 27002.

En la Tabla 38, se hace referencia a la asignación de roles y responsabilidades del personal correspondiente al CONTROL 6, referente a los aspectos organizativos de la seguridad de la información, por ello se presenta un modelo de matriz el cual puede ser tomado como referencia para una futura implementación.

Tabla 38

Asignación de roles y responsabilidades del personal de Administración de Redes de la FISEI

**ASIGNACIÓN DE ROLES Y RESPONSABILIDADES DEL PERSONAL
DE ADMINISTRACIÓN DE REDES DE LA FISEI**

Responsable:

Fecha:

Código:

Nombre	Rol desempeñado	Responsabilidad	Actividad

Nota. En la tabla se muestra una matriz modelo para la asignación de roles y responsabilidades, asociados a la Norma ISO/IEC 27002.

En la Tabla 39, se hace referencia a un informe de daños en los equipos informáticos correspondientes al CONTROL 11, sobre a la seguridad física y ambiental, del literal 11.2 que se enfoca en la seguridad de los equipos, por ello se presenta un modelo de matriz el cual puede ser tomado como referencia para una futura implementación.

Tabla 39

Informe de daños en los equipos de Cómputo

INFORME DE DAÑOS EN LOS EQUIPOS DE CÓMPUTO	
Fecha:	Código del informe:
Responsable del Equipo:	
Teléfono:	
Departamento al que pertenece:	
Código del equipo:	
DETALLE DEL PROCESO	
Hardware	
Descripción del daño	
Como se identificó el daño	
Consecuencias del daño	
Acciones a realizar	

Nota. En la tabla se muestra una matriz modelo para un informe de daños en los equipos de cómputo, asociados a la Norma ISO/IEC 27002.

En la Tabla 40, se hace una referencia a un proceso para realizar el respaldo de información correspondiente al CONTROL 12, referente a la seguridad en la operativa, del literal 12.3

enfocado en las copias de seguridad, por ello se presenta un modelo de matriz el cual puede ser tomado como referencia para una futura implementación.

Tabla 40

Registro de proceso de Backup para el respaldo de información.

PROCESO PARA REALIZAR EL RESPALDO DE INFORMACIÓN	
Código del proceso:	
Fecha:	
Departamento al que pertenece:	
RESPONSABLE	
Apellidos y Nombres:	
Cargo:	
Correo electrónico:	
Teléfono:	
TIPO DE INFORMACIÓN A RESPALDAR	
Fuente de datos: (Carpetas, documentos de office, Base de datos, Archivos del sistema, Grabaciones, etc.)	
Respaldo alojado en unidades compartidas: (Especificar la ruta)	
Indicar los archivos a los cuales se les realizará el respaldo: (Listar archivos a respaldarse)	
INFORMACIÓN DEL SERVIDOR A RESPALDAR	
Nombre del Servidor:	
Dirección IP del Servidor:	
Sistema Operativo del Servidor:	
Tipo de Respaldo:	
Tamaño Información a respaldar MB, GB, TB:	
DETALLE DEL RESPALDO	
Tipo del Respaldo:	
Frecuencia con la que se hace el Respaldo:	
Horario de respaldo:	

Nota. En la tabla se muestra una matriz modelo para realizar el respaldo de información, asociados a la Norma ISO/IEC 27002.

En la Tabla 41, se hace una referencia a un proceso para registrar un informe de utilización de antivirus en los equipos informáticos correspondiente al CONTROL 12, referente a la seguridad en la operativa, del literal 12.2 enfocado a la protección contra código malicioso,

por ello se presenta un modelo de matriz el cual puede ser tomado como referencia para una futura implementación.

Tabla 41

Informe de utilización del antivirus en los equipos informáticos

INFORME DE UTILIZACIÓN DE ANTIVIRUS EN LOS EQUIPOS

Fecha:

Código del informe:

Nombre del Equipo:	
Código del equipo:	
Teléfono:	
Dirección IP:	
Sistema Operativo:	
Usuario del equipo:	
Departamento:	
Tipo de Antivirus instalado:	
Tipo de Licenciamiento:	
¿Protección en Tiempo real?	
¿Actualización Automática?	

OBSERVACIONES:

Nota. En la tabla se muestra una matriz modelo para realizar un informe de utilización de antivirus en los equipos, asociados a la Norma ISO/IEC 27002.

En la Tabla 42, se hace una referencia a un proceso para registrar un informe de evaluación de las unidades de almacenamiento correspondiente al CONTROL 8, referente a la gestión de activos, del literal 8.3 enfocado en el manejo de los soportes de almacenamiento, por ello se presenta un modelo de matriz el cual puede ser tomado como referencia para una futura implementación.

Tabla 42

Informe de evaluación de las unidades de almacenamiento

INFORME DE EVALUACIÓN DE LAS UNIDADES DE ALMACENAMIENTO

Responsable del registro:

Teléfono de la persona a cargo:

Fecha del registro:

Código del registro:

DATOS GENERALES

Departamento al que pertenece:	
Código del Equipo:	
Nombre del Equipo:	
Dirección IP:	
Sistema Operativo:	

DATOS DEL FUNCIONARIO

Apellido y Nombre del funcionario:	
Cargo desempeñado:	
Correo institucional:	
Teléfono:	

EVALUACIÓN

Tipo de Unidad de Almacenamiento:	
Tipo de Antivirus instalado:	
Tiempo de evaluación:	
¿Se encontró algún tipo de virus?	
Procedimiento que se realizó:	

OBSERVACIONES:

Nota. En la tabla se muestra una matriz modelo para realizar un de evaluación de las unidades de almacenamiento en los equipos informáticos, asociados a la Norma ISO/IEC 27002.

En la Tabla 43, se hace una referencia a un proceso para registrar un informe de instalación del software correspondiente al CONTROL 12, referente a la seguridad en la operativa, del literal 12.5.1 enfocado en la instalación del software en sistemas en producción, por ello se

presenta un modelo de matriz el cual puede ser tomado como referencia para una futura implementación.

Tabla 43

Informe de instalación de Software

INFORME DE INSTALACIÓN DEL SOFTWARE

Fecha:

Código del informe:

RESPONSABLE DEL EQUIPO

Apellidos y Nombres:	
Cargo del funcionario:	
Correo electrónico:	
Departamento al que pertenece:	
Teléfono:	

RESPONSABLE DE LA INSTALACIÓN

Apellidos y Nombres:	
Cargo del funcionario:	
Correo electrónico:	
Teléfono:	

DATOS DEL EQUIPO INFORMÁTICO

Marca del Equipo:	
Modelo del Equipo:	
Serie del Equipo:	
Código del Equipo:	

DETALLES DEL SOFTWARE

CARACTERÍSTICAS	DESCRIPCIÓN
Nombre de Software:	
Versión del Software:	
Fabricante:	
Nº de serie	
Fecha de instalación:	
Software licenciado/libre:	
Tipo:	

Plataforma:	
Lenguaje de programación:	
Cuenta con Manual de Usuario:	

Nota. En la tabla se muestra una matriz modelo para realizar un informe de instalación de Software en los equipos informáticos, asociados a la Norma ISO/IEC 27002.

En la Tabla 44, se hace una referencia a un proceso para registrar un informe de gestión de la seguridad de las redes y de los servidores correspondiente al CONTROL 13, referente a la seguridad en las telecomunicaciones, del literal 13.1 enfocado en la gestión de la seguridad en las redes, por ello se presenta un modelo de matriz el cual puede ser tomado como referencia para una futura implementación.

Tabla 44

Informe de instalación de Software

INFORME DE GESTIÓN DE LA SEGURIDAD DE LAS REDES Y DE LOS SERVIDORES

Fecha:

Código del Informe:

GESTIÓN EN LA SEGURIDAD DE LA RED	
Tipo de topología en la red	
Funcionamiento de la NAT	
Herramienta utilizada en el monitoreo de la red	
¿Presencia de Antivirus?	
¿Presencia de Firewall en los equipos?	
¿Existen normas en el Firewall?	
¿Escaneo de la Red LAN?	
¿Cuenta con un servidor Proxy?	
GESTIÓN DE LA SEGURIDAD DE LOS SERVIDORES	
Dirección IP del Servidor	
Sistema Operativo	
¿Escaneo de puertos en el servidor?	
Herramienta usada en el escaneo de puertos	

Resultados del escaneo de puertos	
Medidas a realizar con los resultados	
Escaneo de los servidores	
Herramienta usada en el escaneo de servidores	
Resultados del escaneo de los servidores	
Medidas a realizar con los resultados	

OBSERVACIONES

Nota. En la tabla se muestra una matriz modelo para realizar un informe de gestión de la seguridad de las redes y de los servidores en los equipos informáticos, asociados a la Norma ISO/IEC 27002.

En la Tabla 45, se hace una referencia a un proceso para registrar un formulario de creación de usuarios y contraseñas solicitudes de acceso a dispositivos y sistemas de información correspondiente al CONTROL 9, referente al control de acceso, del literal 9.1.2 enfocado en el control de acceso a las redes y servicios asociados, por ello se presenta un modelo de matriz el cual puede ser tomado como referencia para una futura implementación.

Tabla 45

Formulario para la Creación de Usuarios y Contraseñas

**FORMULARIO DE CREACIÓN DE USUARIOS Y CONTRASEÑAS
SOLICITUDES DE ACCESO A DISPOSITIVOS Y SISTEMAS DE
INFORMACIÓN**

Fecha:

Código:

DATOS GENERALES

Departamento al que pertenece:	
--------------------------------	--

DATOS DEL FUNCIONARIO

Apellido y Nombre del funcionario	
-----------------------------------	--

Cargo desempeñado:	
--------------------	--

Correo:	
---------	--

Teléfono:	
-----------	--

**PERFIL DEL FUNCIONARIO A CREAR PARA LOS DISPOSITIVOS
INFORMÁTICOS**

Dirección IP del dispositivo:	
-------------------------------	--

Sistema Operativo:	
--------------------	--

Funcionario:	
--------------	--

Contraseña:	
-------------	--

**PERFIL DEL FUNCIONARIO A CREAR PARA LOS SISTEMAS DE
INFORMACIÓN**

Sistema de Información:	
-------------------------	--

Funcionario:	
Contraseña:	
¿Tiene doble Factor de Autenticación?	
¿Cuenta con autenticación través de un teléfono móvil o correo electrónico?	
OBSERVACIONES	

Nota. En la tabla se muestra una matriz modelo para realizar un formulario para la creación de usuarios y contraseñas en los equipos informáticos, asociados a la Norma ISO/IEC 27002.

En la Tabla 46, se hace una referencia a un proceso para registrar un formulario de creación de usuarios y contraseñas solicitudes de acceso a dispositivos y sistemas de información correspondiente al CONTROL 9, referente al control de acceso, del literal 9.2 enfocado en la gestión de acceso de usuario, por ello se presenta un modelo de matriz el cual puede ser tomado como referencia para una futura implementación.

Tabla 46

Formulario para el Acceso de recursos compartidos en red

PERMISOS PARA EL ACCESO A LOS RECURSOS COMPARTIDOS EN LA RED			
Fecha:			
Código del informe:			
DATOS DEL RESPONSABLE			
Departamento al que pertenece:			
Apellidos y Nombres:			
Teléfono y extensión del departamento:			
Correo:			
DATOS DEL SOLICITANTE			
Departamento al que pertenece:			
Apellidos y Nombres:			
Teléfono y extensión del departamento:			
Correo:			
DATOS DEL RECURSO			
Dirección IP del equipo:			
Nombre del recurso:			
Ruta a la cual se solicita acceder:			
DATOS DE LOS USUARIOS			
N°	Apellidos y Nombres	Permisos Requeridos	
		<input type="checkbox"/> Lectura <input type="checkbox"/> Denegar	<input type="checkbox"/> Escritura
		<input type="checkbox"/> Lectura <input type="checkbox"/> Denegar	<input type="checkbox"/> Escritura

Nota. En la tabla se muestra una matriz modelo para realizar un Formulario para el Acceso de recursos compartidos en red en los equipos informáticos, asociados a la Norma ISO/IEC 27002.

En la Tabla 47, se hace una referencia a un proceso para el registro de Sistemas de Información correspondiente al CONTROL 8, referente a la gestión de activos, del literal

8.1.2 enfocado en la propiedad de los activos, por ello se presenta un modelo de matriz el cual puede ser tomado como referencia para una futura implementación.

Tabla 47

Formulario para el registro de Sistemas de Información

REGISTRO DE SISTEMAS DE INFORMACIÓN	
Fecha:	
Código del formulario:	
ATRIBUTO	DETALLE
Nombre del sistema	
Nombre del servicio	
Tipo de sistema	
Nombre del Proveedor	
Tipo de licencia	
Fecha de expiración de la licencia	
Tipo de Plataforma	
Ubicación del equipo	
Tipo de gestor de base de datos	
Responsable de la Base de Datos	

Nota. En la tabla se muestra una matriz modelo para realizar un registro de sistemas de información sobre los equipos informáticos, asociados a la Norma ISO/IEC 27002.

En la Tabla 48, se hace una referencia a un proceso para proceder con la categorización de la información correspondiente al CONTROL 8, referente a la gestión de activos, del literal 8.2 enfocado en la clasificación de la información, por ello se presenta un modelo de matriz el cual puede ser tomado como referencia para una futura implementación

Tabla 48

Categorización de la Información

CATEGORIZACIÓN DE LA INFORMACIÓN

ha:

ligo del Formulario:

REGISTRO INFORMACIÓN DEL ACTIVO					NIVEL DE CRITICIDAD					
Nombre del Activo	Descripción Activo	Sistema Involucrado	Nivel de Confidencialidad	Custodio del Activo	Confidencialidad	Integridad	Disponibilidad	Valor	Nivel de Tasación	Fecha Registro

Nota. En la tabla se muestra una matriz modelo para realizar una categorización de información sobre los equipos informático, asociados a la Norma ISO/IEC 27002.

ACTUAR

En este apartado se sugiere implementar el modelo de gestión de seguridad de la información propuesta, ya que consta con información actual y veras de los problemas reales que presenta la FISEI. Este proceso de gestión de la seguridad se lo debe ir desarrollando constantemente para adquirir un modelo de madurez óptimo para garantizar la confidencialidad, integridad y disponibilidad de los datos. Ejecutar procedimientos de seguimiento y revisión constante de los controles de la ISI/IEC 27002.

FASE 4: CRONOGRAMA

Tabla 49

Cronograma de actividades

ACTIVIDADES	JULIO				AGOSTO				SEPTIEMBRE			
	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
Análisis de la situación actual de la FISEI a través de las directrices de aplicabilidad.	■	■	■	■								
Interpretación de los resultados obtenidos en las directrices de aplicabilidad.				■	■	■						
Aplicar un escaneo de puertos con las herramientas NMAP y Nessus.					■	■	■					
Identificar los resultados del análisis de vulnerabilidades del listado de activos informáticos críticos.						■	■	■				
Elaborar políticas de Seguridad de la Información basados los controles de la norma ISO/IEC 27002.								■	■	■		
Plantear acciones frente a los tipos de riesgo proponiendo un conjunto de tablas para verificar el estado de los controles.										■	■	■
Modelar el sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27002.												
Desarrollar la propuesta de solución en el ámbito de un caso de estudio en la FISEI de la UTA.	■	■	■	■	■	■	■	■	■	■	■	■

Nota. En la tabla se muestra el cronograma de actividades correspondiente al desarrollo de la propuesta y como se ha ido trabajando cronológicamente.

Conclusiones

- Se evidenció la existencia de vulnerabilidades en los diferentes activos críticos de la FISEI, mismos que albergan gran cantidad de información de suma importancia, que se encuentran inmersos a cualquier ataque informático afectando así la buena imagen de la institución.
- Se elaboró un modelo de gestión de seguridad de la información de acuerdo a los controles establecidos en la norma ISO/IEC 27002, identificando las necesidades de la FISEI, mismo ayudará a gestionar el manejo de la seguridad de la información a través de políticas que conllevan a garantizar la confidencialidad, integridad y disponibilidad de la misma.
- Se desarrolló la propuesta de solución planteada en el presente proyecto de investigación cumpliendo con los objetivos trazados, permitiendo contar con un modelo de gestión de seguridad de la información el cual permite poner en marcha el caso de estudio al trabajar con datos reales de la FISEI de la UTA.

Recomendaciones

- Se recomienda que, la implementación de la normativa de la seguridad de la información se considere todos los controles de la ISO/IEC 27002, cumpliendo el mayor nivel de aceptación y su correcta documentación.
- Es recomendable que la FISEI cuente con un SGSI (Sistema de Gestión de Seguridad de la Información), con el objetivo de proteger los activos informáticos garantizando un marco de protección organizativo respecto a la confidencialidad, integridad y disponibilidad de la información.
- Realizar la implementación de la propuesta en el presente trabajo de investigación, permitiendo establecer las buenas prácticas de la norma ISO/IEC 27002, adoptando la metodología Deming, ya que dicha metodología permite contar con una mejora continua, garantizando el cumplimiento de las fases del ciclo PDCA.
- Ejecutar pruebas de penetración tanto interna como externa en la red, a través del uso de aplicaciones disponibles en el mercado, esto con el objetivo de identificar

vulnerabilidades, permitiendo así proponer nuevas políticas que cubran las falencias encontradas.

- Los servidores públicos de la FISEI de la UTA no se encuentran capacitados con respecto a la importancia que se le debe dar al tema de gestión de la seguridad de la información, a lo cual se recomienda una mayor socialización frente a los riesgos, permitiendo prevenir, resguardar y proteger la información de la institución.