



REPÚBLICA DEL ECUADOR

**VICERRECTORADO DE INVESTIGACIÓN Y
POSGRADO**

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN

TÍTULO DEL PROYECTO:

**Evaluación de la seguridad informática bajo las normas
ISO/IEC 27001 en la infraestructura tecnológica de la
Universidad Estatal de Milagro**

TUTOR

RAMIREZ ANORMALIZA RICHARD IVAN

AUTOR

LUIS CASTILLO SALVATIERRA

MILAGRO, 2022



VICERRECTORADO DE INVESTIGACIÓN Y POSGRADO

Milagro, 31 octubre, 2021

CERTIFICACIÓN DE ACEPTACIÓN DEL TUTOR

En calidad de Tutor del Proyecto de Investigación, nombrado por el Comité Académico del Programa de Maestría en Tecnologías de la Información de la Universidad Estatal de Milagro.

CERTIFICO

Que he analizado el Proyecto de Investigación con el tema **EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA BAJO LAS NORMAS ISO/IEC 27001 EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIVERSIDAD ESTATAL DE MILAGRO**, elaborado por **CASTILLO SALVATIERRA LUIS ENRIQUE**, el mismo que reúne las condiciones y requisitos previos para ser defendido ante el tribunal examinador, para optar por el título de **MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN**.



firmado electrónicamente por:
RICHARD IVAN
RAMIREZ ANORMALIZA

RAMIREZ ANORMALIZA RICHARD IVAN

C.I: 1203238132



DECLARACIÓN DE AUTORÍA DE LA INVESTIGACIÓN

El autor de esta investigación declara ante el Comité Académico del Programa de Maestría en Tecnologías de la Información de la Universidad Estatal de Milagro, que el trabajo presentado es de mi propia autoría, no contiene material escrito por otra persona, salvo el que está referenciado debidamente en el texto; parte del presente documento o en su totalidad no ha sido aceptado para el otorgamiento de cualquier otro título de una institución nacional o extranjera.

**LUISENRIQUE
CASTILLO
SALVATIERRA**

Firmado digitalmente por LUIS ENRIQUE
CASTILLO SALVATIERRA
Nombre de reconocimiento (DN):
cn=LUIS ENRIQUE CASTILLO
SALVATIERRA,
serialNumber=151021114632,
ou=ENTIDAD DE CERTIFICACION DE
INFORMACION, o=SECURITY DATA S.A.
2, c=EC
Fecha: 2023.04.27 16:54:23 -05'00'

**CASTILLO SALVATIERRA LUIS ENRIQUE
C.I: 1203238132**

VICERRECTORADO DE INVESTIGACIÓN Y POSGRADO
DIRECCIÓN DE POSGRADO
CERTIFICACIÓN DE LA DEFENSA

El TRIBUNAL CALIFICADOR previo a la obtención del título de **MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN**, presentado por **ING. CASTILLO SALVATIERRA LUIS ENRIQUE**, otorga al presente proyecto de investigación denominado "EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA BAJO LAS NORMAS ISO/IEC 27001 EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIVERSIDAD ESTATAL DE MILAGRO", las siguientes calificaciones:

| | |
|-----------------------|------------------|
| TRABAJO DE TITULACION | 55.67 |
| DEFENSA ORAL | 39.00 |
| PROMEDIO | 94.67 |
| EQUIVALENTE | Muy Bueno |



Firmado electrónicamente por:
ANA EVA CHACON LUNA

Mgti. CHACON LUNA ANA EVA
PRESIDENTE/A DEL TRIBUNAL



Firmado electrónicamente por:
**JAVIER RICARDO
BERMEO PAUCAR**

Mgti. BERMEO PAUCAR JAVIER RICARDO
VOCAL



Firmado electrónicamente por:
**RICAUTER
MOISES LOPEZ
BERMUDEZ**

Analista LOPEZ BERMUDEZ RICAUTER MOISES
SECRETARIO/A DEL TRIBUNAL



CESIÓN DE DERECHOS DE AUTOR

Doctor
ING. FABRICIO GUEVARA VIEJÓ, PhD
Rector de la Universidad Estatal de Milagro

Presente.

Mediante el presente documento, libre y voluntariamente procedo a hacer entrega de la Cesión de Derecho del Autor al Trabajo realizado como requisito previo para la obtención de mi Título de Cuarto Nivel, cuyo tema fue **EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA BAJO LAS NORMAS ISO/IEC 27001 EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIVERSIDAD ESTATAL DE MILAGRO**, elaborado por **CASTILLO SALVATIERRA LUIS ENRIQUE** y que corresponde al Vicerrectorado de Investigación y Posgrado.

LUIS ENRIQUE
CASTILLO
SALVATIERRA

Firmado digitalmente por LUIS ENRIQUE
CASTILLO SALVATIERRA
Nombre de reconocimiento (DN): cn=LUIS
ENRIQUE CASTILLO SALVATIERRA,
serialNumber=151021114632, ou=ENTIDAD
DE CERTIFICACION DE INFORMACION,
o=SECURITY DATA S.A. 2, c=EC
Fecha: 2023.04.27 16:54:52 -05'00'

CASTILLO SALVATIERRA LUIS ENRIQUE
C.I: 1203238132

DEDICATORIA

Este proyecto de maestría es un logro en mi vida profesional va dedicado a mi familia por guiarme en todo momento, y enseñarme que en la vida todo se gana con esfuerzo, por dar el apoyo en cada paso de mi vida y estar presentes, para enseñarme que cada objetivo que me proponga hay que lucharlo hasta conseguirlo y principalmente por forjarme a llegar hasta este peldaño.

Este trabajo está dedicado a todas las personas que se esfuerzan día a día para cumplir sus metas y propósitos.

Atentamente,

Luis Castillo Salvatierra

AGRADECIMIENTOS

A la Universidad Estatal de Milagro que me brindó una educación superior de calidad, en el cual he forjado gran parte de mi conocimiento y vida profesional.

A Dios y a mi Madre Bélgica Salvatierra, mi padre Luis A. Castillo y mi hermana Elizabeth Castillo que me han acompañado en cada paso de mi vida.

A mi novia Mayra D'Armas por incentivar-me a retomar los estudios y darme la confianza para seguir mejorando como profesional.

A la directora de tecnología de la información y comunicaciones Kerly Palacios Zamora por su gentil apoyo y acceso a la información para la elaboración de este proyecto maestrante.

A mi tutor Richard Ramírez Anormaliza por su completo apoyo durante el desarrollo de la tesis.

A todo mi equipo de trabajo del área de Operaciones por su gran apoyo y ardua predisposición laboral.

Atentamente,

Luis Castillo Salvatierra

RESUMEN

El proyecto maestrante tuvo como finalidad detectar las vulnerabilidades de la Universidad Estatal de Milagro con el fin de mejorar la infraestructura tecnológica, basado en la norma ISO/IEC 27001 con el propósito de disminuir los riesgos en los sistemas de información de la institución. Se aplicó la metodología en función de los objetivos establecidos, determinación de la situación actual de los procesos, recursos, infraestructura, componentes de hardware, software y sobre todo la información de la dirección de tecnología de la información. Investigación de los componentes de hardware que soportan la infraestructura tecnológica. Diseño de un cuestionario de preguntas tipo checklist estructuradas y basadas en los diferentes componentes de la norma aplicadas. Evaluación de los riesgos en base a las vulnerabilidades detectadas. Aplicación de la metodología Análisis Modal de Fallos y Efectos (AMFE), mediante la identificación del nivel de riesgo de cada componente, lo cual permitió tomar acciones de mitigación con respecto a la integridad de la información. Y, por último, planteamiento de un listado de recomendaciones de acuerdo con las vulnerabilidades encontradas, orientadas a la mejora de la seguridad de la información.

PALABRAS CLAVES

UNEMI, Gestión de la información, Seguridad de la información, AMFE, ISO/IEC 27001, vulnerabilidades de la infraestructura tecnológica.

ABSTRACT

The purpose of the master project was to detect the vulnerabilities of the State University of Milagro in order to improve the technological infrastructure, based on the ISO/IEC 27001 standard with the purpose to reduce the risks in the institution's information systems. The methodology was applied according to the established objectives, determination of the current situation of the processes, resources, infrastructure, hardware components, software and especially the information of the information technology management. Research of the hardware components that support the technological infrastructure. Design of a questionnaire of structured checklist questions based on the different components of the standard applied. Risk assessment based on detected vulnerabilities. Application of the Failure and Effect Mode Analysis (FMEA) methodology, by identifying the risk level of each component, which allowed mitigation actions to be taken with respect to the integrity of the information. And, finally, propose a list of recommendations according to the vulnerabilities found, aimed at improving information security.

KEYWORDS

UNEMI, Information Management, Information Security, FMEA, ISO/IEC 27001, vulnerabilities in technological infrastructure.

ÍNDICE GENERAL

| | |
|---|-----|
| RESUMEN | I |
| PALABRAS CLAVES..... | I |
| ABSTRACT | II |
| KEYWORDS | II |
| ÍNDICE GENERAL | III |
| INDICE DE FIGURAS | V |
| INDICE DE TABLAS..... | VI |
| CAPÍTULO 1..... | 1 |
| 1. INTRODUCCIÓN..... | 1 |
| 1.1. Planteamiento del problema | 1 |
| 1.2. Justificación..... | 4 |
| 1.3. Objetivos | 5 |
| 1.4. Alcance | 6 |
| 1.5. Estado del Arte..... | 7 |
| 1.5.1. Antecedente de la investigación..... | 7 |
| 1.5.2. Teoría de Sistema | 8 |
| 1.5.3. Sistemas de Información | 9 |
| 1.5.4. Seguridad Informática | 11 |
| 1.5.5. Infraestructura Tecnológica | 12 |
| 1.5.6. Estándar ISO/IEC 27001 | 13 |
| CAPÍTULO 2..... | 15 |
| 2. METODOLOGÍA | 15 |

| | | |
|---|--|-----------|
| 2.1 | Infraestructura de red y componentes de hardware | 15 |
| 2.2 | Infraestructura de red y componentes de software..... | 19 |
| 2.3 | Método de desarrollo | 23 |
| 2.4 | Fase para la obtención de evidencia | 24 |
| CAPÍTULO 3..... | | 28 |
| 3. | EVALUACION, AMENAZAS Y VULNERABILIDADES..... | 28 |
| 3.1 | Evaluación y Amenazas | 33 |
| CAPÍTULO 4..... | | 13 |
| 4. | CONCLUSIONES Y TRABAJO FUTURO | 16 |
| 4.1 | CONCLUSIONES..... | 17 |
| 4.2 | Recomendaciones de mejora de la seguridad informática UNEMI..... | 17 |
| BIBLIOGRAFÍA | | 19 |
| ANEXO 1: Solicitud de ingreso a la Dirección TIC para el levantamiento de información..... | | 22 |
| ANEXO 2: Solicitud de aceptación por la Dirección TIC para el levantamiento de información..... | | 23 |
| ANEXO 3: Aplicado al departamento tecnológico basado en la Norma ISO/IEC 27001. | | 24 |

INDICE DE FIGURAS

| | |
|--|----|
| Figure 1. Total de estudiantes matriculados en pregrado..... | 1 |
| Figura 2. Procesos de un SGSI | 8 |
| Figura 3. Proveedores de la red UNEMI. | 16 |
| Figura 4. Router Fortinet Cisco. | 16 |
| Figura 5. Swtich principal. | 17 |
| Figura 6. Servidor DHCP. | 18 |
| Figura 7. Antena wifi | 18 |
| Figura 8. Esquema de infraestructura de red de la red UNEMI. | 19 |
| Figura 9. Firewall Fortinet UNEMI..... | 21 |
| Figura 10. Controladora de antenas wifi UNEMI..... | 22 |
| Figura 11. Software de monitoreo Zabbix UNEMI. | 22 |
| Figura 12. Administrador de direcciones ip PHPIPAM..... | 23 |
| Figura 13. Total de vulnerabilidades..... | 31 |
| Figura 14 Total de vulnerabilidades que No Cumplen | 32 |
| Figura 15 Total de Vulnerabilidades por cada componente..... | 32 |

INDICE DE TABLAS

| | |
|--|----|
| Tabla 1. Evolución de la función de los sistemas de información..... | 10 |
| Tabla 2 Preguntas del componente Inventario Activo | 25 |
| Tabla 3 Preguntas del componente Seguridad de los Recursos Humanos | 25 |
| Tabla 4 Preguntas del componente Seguridad Física del Entorno..... | 25 |
| Tabla 5 Preguntas del componente Gestión de Comunicación y de Operación..... | 25 |
| Tabla 6 Preguntas del componente Control de Acceso | 27 |
| Tabla 7 Preguntas del componente Cumplimiento..... | 27 |
| Tabla 8. Calificación del componente Inventario Activo según la norma ISO 27001..... | 28 |
| Tabla 9. Calificación del componente Seguridad Física según la norma ISO 27001 | 29 |
| Tabla 10. Calificación del componente Seguridad de los RRHH según la norma ISO 27001..... | 29 |
| Tabla 11. Calificación del componente gestión de comunicación y operación según la norma ISO 27001. | 30 |
| Tabla 12. Calificación del componente Control de Acceso según la norma ISO 27001. | 30 |
| Tabla 13. Calificación del componente Cumplimiento según la norma ISO 27001 | 30 |
| Tabla 14. Vulnerabilidades en el componente Inventario de Activo | 33 |
| Tabla 15. Vulnerabilidades en el componente Seguridad de los Recursos Humanos. ... | 34 |
| Tabla 16. Vulnerabilidades en el componente Seguridad Física del Entorno..... | 34 |
| Tabla 17. Vulnerabilidades en el componente Gestión de Comunicación y Operación. | 37 |
| Tabla 18. Vulnerabilidades en el componente Control de Acceso | 38 |
| Tabla 19. Vulnerabilidades en el componente Cumplimiento..... | 39 |
| Tabla 20. Porcentaje de Riesgo de componentes de la norma ISO 27001..... | 40 |
| Tabla 21. Matriz de Riesgos basado en el componente Inventario de Activo según norma ISO/IEC 27001..... | 1 |
| Tabla 22. Matriz de Riesgos basado en el componente Seguridad de los Recursos Humanos según norma ISO/IEC 27001. | 2 |
| Tabla 23. Matriz de Riesgos basado en el componente Seguridad Física del Entorno según norma ISO/IEC 27001..... | 3 |
| Tabla 24. Matriz de Riesgos basado en el componente Gestión de Comunicación y Operación según norma ISO/IEC 27001 | 8 |
| Tabla 25. Matriz de Riesgos basado en el componente Control de Acceso según norma ISO/IEC 27001..... | 11 |
| Tabla 26. Matriz de Riesgos basado en el componente Cumplimiento según norma ISO/IEC 27001..... | 12 |

CAPÍTULO 1

1. INTRODUCCIÓN

En los últimos años, el uso de la informática se ha extendido a la mayoría de las actividades profesionales y humanas a nivel mundial, convirtiéndose las redes de comunicación y los sistemas de información (SI) en un factor esencial para el desarrollo económico y social de las naciones (Ramírez Castro & Ortiz Bayona, 2011).

De acuerdo a los datos recabados del sistema académico de la Universidad Estatal de Milagro SGA+ nos presenta la cantidad de estudiantes registrados en admisión, pregrado en las diferentes modalidades (presencial y semipresencial) del periodo mayo a septiembre de 2022 es de 39.630 (Figura 1) de los cuales se encuentran matriculados en pregrado en las Facultades de Ciencia de la Ingeniería (FACI), Educación (FACE), Salud (FACS) y Ciencias Sociales, Educación Comercial y Derecho (FACESECYT), cifra que evidencia la existencia de una gran infraestructura que brinda soporte a una red tecnológica exigente.

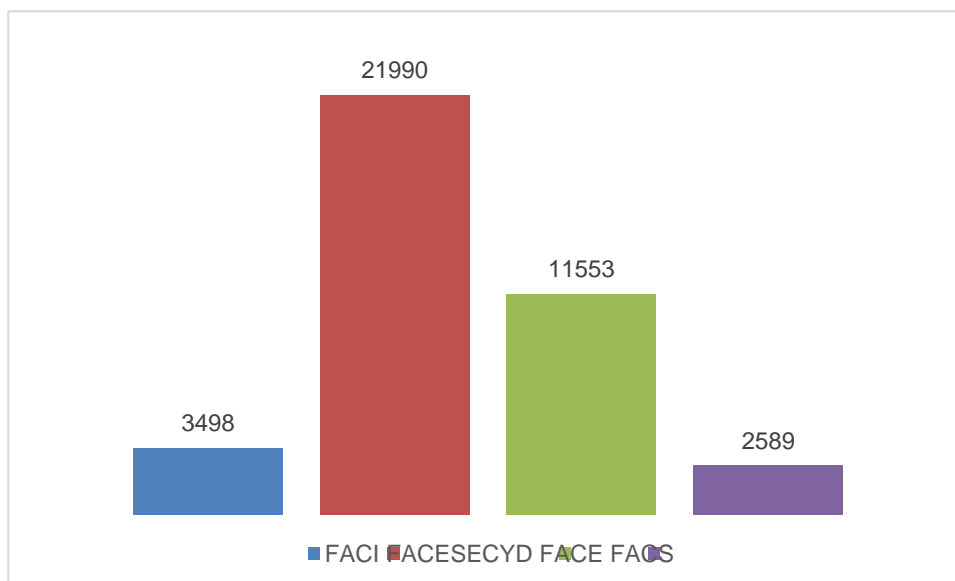


Figure 1. Total de estudiantes matriculados en pregrado.

La seguridad de los datos es un tema delicado y de mucho cuidado para el éxito de la institución. Debido a la pandemia y la implementación de clases virtuales los requerimientos de la institución se vieron en la necesidad de desarrollar varios softwares tales como: tesorería, financiero, nómina de rol de pagos, inventarios, avalúos etc. Por tal razón es de carácter vital que la seguridad de la información garantice su funcionamiento.

Por otro lado, se tienen las amenazas físicas que afectan a la infraestructura tecnológica de las instituciones, teniendo en claro que las infraestructuras tecnológicas son el hardware y software que poseen las entidades. Las amenazas físicas como su nombre lo indica están relacionadas al hardware, en fin, estas amenazas se pueden producir de

forma voluntaria o involuntaria, por ejemplo: un cortocircuito, un robo o un incendio, por tal motivo es importante resguardar la seguridad física de los equipos y sistemas informáticos, ya sea con procedimientos de control, medidas ante amenazas de los recursos, etc.

Los sistemas de información, los datos contenidos en ellas y la información son los activos más valiosos para las organizaciones y se hace necesario brindarles una protección adecuada frente a las posibles intrusiones derivadas de las vulnerabilidades existentes en sus sistemas de seguridad (Solarte, Enriquez, & Benavides, 2015). La Universidad Estatal de Milagro (UNEMI) no está exenta de dicho contexto, y siendo la Institución de Educación Superior (IES) en la Zona 5 con mayor demanda de jóvenes que buscan formarse profesionalmente para lograr insertarse en campo laboral, esta institución se ve en la obligación de mejorar día a día los servicios que brinda a la comunidad universitaria.

Este proyecto maestrante lleva como fin mejorar la seguridad de la información por ende la infraestructura tecnológica aplicando estándares internacionales y best practice con el fin de garantizar la seguridad y confidencialidad de los datos personales, evitar pérdidas, adulteraciones, accesos indebidos que permitan corromper la integridad de la información, ya sean registros de acción humana o del medio tecnológico.

Dado que los procesos administrativos y académicos de la institución están soportado por la internet, y por ende a la infraestructura tecnológica, está sujeto ataques informáticos, tales como: el robo de contenido digital o activos digitales, documentos, calificaciones, test, exámenes, audios, videos o hasta títulos, certificados, diplomas, entre otros. Por lo cual, el propósito de este proyecto es evaluar todos los riesgos que se pueden presentar para brindar una infraestructura tecnológica robusta en la Universidad Estatal de Milagro.

Este proyecto se encuentra basado legalmente por la LOTAIP (Ley Orgánica de Transparencia y Acceso a la información pública) en relación al derecho de acceso a la información relacionada con asuntos públicos (educacion.gob.ec, 2022). El fin de dicho proyecto es centralizar y mejorar la seguridad de la información, basado en las normas ISO 270001 y buenas practicas, el cual salvaguarda el recurso más importante de la institución educativa UNEMI, la información.

Además, se busca el progreso de la Universidad con los datos disponibles, con el fin de obtener alternativas de control que mejoren la confidencialidad de la información y convertir las debilidades en fortalezas que mitiguen los riesgos de la información en los diferentes departamentos.

1.1. Planteamiento del problema

La importante presencia de las tecnologías de información y comunicación y el creciente volumen de información que se maneja dentro de las organizaciones, aumentado a la tendencia cada vez más persistente de estar interconectado, ha traído como consecuencia que las organizaciones se ven expuestas a una cantidad de retos y amenazas que son cada vez más sofisticadas y que les obliga a proteger la información por ser uno de sus activos más valiosos (Valduciel, 2014).

En el ámbito educativo, el uso de las herramientas tecnológicas se ha intensificado, los últimos acontecimientos han forzado un cambio acelerado en las modalidades de estudio, lo que ha obligado a las instituciones educativas a adaptarse a las nuevas clases virtuales, estar en continuo desarrollo para fortalecer la infraestructura tecnológica, y así satisfacer las actuales necesidades a las que se enfrenta el sistema educativo.

No obstante, la incorporación de las tecnologías de la información y comunicación (TIC) como soporte a los procesos académicos y administrativos de las instituciones hace imprescindible tomar en cuenta los temas de seguridad. El uso de las TIC no solamente facilita lograr el alcance de los objetivos y metas de la organización, sino que trae como consecuencia el riesgo inherente a ellas, es decir la posibilidad de que una debilidad sea aprovechada por una amenaza y sus consecuencias: divulgación, modificación, pérdida o interrupción de información sensible (Mendoza & Lorenzana, 2013).

De acuerdo a lo antes mencionado la seguridad de los datos es de carácter vital para el éxito de toda institución, lo cual recae en la responsabilidad de TIC. Por tal motivo desde hace un tiempo atrás se han implementado medidas de seguridad como lo es el control de acceso y firewalls además de implementar algunas políticas de seguridad para tener una idea más clara del manejo de la información y los recursos.

Ante los requerimientos de la institución de cada departamento existió la necesidad de desarrollar un software para la institución el cual es SGA+ Sistema de Gestión Académica el cual entre sus funciones importantes se encuentran el sistema financiero, rentas, catastros, avalúos, tesorería, rol de pagos e inventarios de activos fijos, estos son procesos de índole tipo crítico en el nivel de seguridad, por tal motivo la preocupación para la Universidad Estatal de Milagro que dichos sistemas no cuenten con la seguridad que se requiere para su funcionalidad.

La realidad informática es que todo sistema posee un conjunto de debilidades o vulnerabilidades por tal motivo es necesario hacer un escaneo de vulnerabilidades que ayuden a detectar y a su vez mejorar los sistemas informáticos. Por esta razón este trabajo de tesis maestrante conlleva un diagnóstico de los procesos que se aplican en la Universidad Estatal de Milagro (UNEMI) con el fin de contribuir un aporte para seguridad de la información de la institución, promoviendo la innovación tanto de softwares o hardware de los diferentes sistemas informáticos.

Es relevante señalar la importancia de identificar las amenazas y posibles ataques al que se enfrentan las infraestructuras tecnológicas. Como se ha mencionado anteriormente pueden existir tres tipos de amenazas a las que se enfrentan los sistemas informáticos: humanas, lógicas y físicas, siendo relevante conocerlas y estudiarlas para fortalecer los sistemas y así contar con la capacidad para contrarrestar estos ataques informáticos. Se deben identificar las amenazas humanas que afectan a las infraestructuras tecnológicas, como pueden ser los hackers (personas que ingresan a los sistemas cuando no están

autorizados), que, aunque la mayoría no tienen intenciones maliciosas sino más bien curiosidad o deseo de aprender, no se debe de tomar a la ligera este tipo de acciones ya que su sola intrusión representa una peligrosa amenaza, por lo que puede ocasionar daños no intencionados. También se encuentran los crackers (conocido como hacker dañino), que tratan de penetrar en el sistema con el fin de ocasionar daños o robar información, este tipo de personas suelen ser peligrosas ya que poseen el conocimiento, la experiencia y las herramientas necesarias para vulnerar los sistemas. Por lo cual nos llevan a tener las siguientes interrogantes:

- ¿Cómo puede la Universidad Estatal de Milagro contar con la seguridad informática que le permita afrontar de manera satisfactoria los diferentes riesgos, así como prevenirlos, para mantener segura la infraestructura tecnológica?
- ¿Cuáles son las amenazas humanas que pueden vulnerar la infraestructura tecnológica de la institución?
- ¿Cuáles son los riesgos de las amenazas lógicas que se pueden evidenciar, así como las diferentes amenazas físicas que se puedan presentar para violar la seguridad de la información?
- ¿Cómo evitar que usuarios no autorizados puedan acceder a equipo o información confidencial dentro de la infraestructura tecnológica?
- ¿Cuáles son los recursos de la infraestructura tecnológica más críticos o de mayor prioridad dentro de la organización que pueden ser afectados por un problema de seguridad?
- ¿De qué forma se podría generar conciencia en la comunidad universitaria acerca de temas de seguridad informática?

De esta manera establecer un análisis más amplio y claro de los posibles escenarios a los que se enfrentan las actividades administrativas y académicas, y qué puede hacerse para evitar riesgos y ataques a la infraestructura tecnológica.

A partir de la situación descrita, surgió la necesidad de desarrollar esta investigación con el propósito de evaluar la seguridad informática, bajo la Norma ISO/IEC 27001, en la infraestructura tecnológica de la Universidad Estatal de Milagro, lo que permitirá conocer el nivel de impacto que pueden tener la ocurrencia de las amenazas en cada activo de la infraestructura tecnológica, minimizar los riesgos existentes y, por ende, ayudar a fortalecer la confidencialidad, integridad y disponibilidad de la información.

1.2. Justificación

En el Ecuador la ciberseguridad es un tema no muy desconocido hoy en día, ya que en los últimos años un cierto porcentaje de empresas públicas, privadas y sobre todo instituciones educativas han sufrido ataques cibernéticos debido a su débil infraestructura tecnológica, poniendo en riesgo la integridad de la información. Esto ocasionado por la poca importancia que se le dedica a un correcto sistema de seguridad, que controle la vulnerabilidad de sus equipos tecnológicos, haciéndolos blancos fáciles de todo tipo de ataques cibernéticos.

Según Miranda Cairo y otros (2016), los ataques más importantes se deben principalmente a aspectos como las vulnerabilidades de software, malware, dispositivos móviles, personal interno y hackers, los cuales acaparan alrededor del 69% de causas de ataques cibernéticos. Sin embargo, existen diferentes tipos de amenazas que afectan a los sistemas de información entre las que se encuentran las humanas que son la principal fuente de amenaza a la que se enfrentan las infraestructuras tecnológicas, ya sea por actos malintencionados, actos negligentes o también falta de un control adecuado sobre los sistemas, lo que conlleva a utilizar más recursos para controlarlos y contrarrestarlo. Además, están las amenazas lógicas que también afectan de forma gradual a las infraestructuras tecnológicas, estas amenazas lógicas representan todo tipo de programas que de alguna manera u otra intentan dañar o vulneran los sistemas, comúnmente se conocen como softwares maliciosos, también llamados malware, por ello es importante mantener un constante análisis de riesgos para evitar este tipo de ataques.

Es relevante señalar la importancia de identificar las amenazas y posibles ataques al que se enfrentan las infraestructuras tecnológicas. Como se ha mencionado anteriormente pueden existir tres tipos de amenazas a las que se enfrentan los sistemas informáticos: humanas, lógicas y físicas, siendo relevante conocerlas y estudiarlas para fortalecer los sistemas y así contar con la capacidad para contrarrestar estos ataques informáticos. Se deben identificar las amenazas humanas que afectan a las infraestructuras tecnológicas, como pueden ser los hackers (personas que ingresan a los sistemas cuando no están autorizados), que, aunque la mayoría no tienen intenciones maliciosas sino más bien curiosidad o deseo de aprender, no se debe de tomar a la ligera este tipo de acciones ya que su sola intrusión representa una peligrosa amenaza, por lo que puede ocasionar daños no intencionados. También se encuentran los crackers (conocido como hacker dañino), que tratan de penetrar en el sistema con el fin de ocasionar daños o robar información, este tipo de personas suelen ser peligrosas ya que poseen el conocimiento, la experiencia y las herramientas necesarias para vulnerar los sistemas.

Además, se deben analizar las amenazas lógicas a las que se enfrenta la infraestructura tecnológica, teniendo en cuenta las posibles amenazas lógicas que pueden ingresar a nuestros sistemas a causar daños, entre estos los malware y los bugs o agujeros. Así como establecer las amenazas físicas dentro de la infraestructura, toda entidad o institución educativa debe contar con controles de seguridad que permitan prevenir daños físicos en la institución, por ello, es importante contar con manuales de seguridad informática que permita salvaguardar la integridad de la infraestructura informática.

Una manera efectiva de descubrir estas vulnerabilidades y amenazas existentes es iniciando los procesos diagnósticos que permitan establecer el estado actual de la seguridad dentro de la organización, teniendo en cuenta la normativa ISO 27001 ya que indica un análisis y evaluación de riesgos (Solarte, Enriquez, & Benavides, 2015).

El presente proyecto tiene como propósito realizar una evaluación de la seguridad informática de la red basado en las normas ISO/IEC 27001 en la infraestructura tecnológica de la Universidad Estatal de Milagro, con el propósito de mejorar la seguridad informática de los recursos tecnológicos, con el fin de evitar, prevenir, detectar posibles ataques y amenazas que afecten a la Universidad, así como la recomendación de políticas de seguridad para la centralización y control de la información de tal.

1.3. Objetivos

1.3.1. Objetivo General

Evaluar la seguridad informática, bajo la Norma ISO/IEC 27001, en la infraestructura tecnológica de la Universidad Estatal de Milagro.

1.3.2. Objetivos Específicos

- Identificar mecanismos de seguridad informática para evitar que usuarios no autorizados puedan acceder a equipos o información dentro de la infraestructura tecnológica de la Universidad Estatal de Milagro.
- Reconocer los recursos de la infraestructura tecnológica de la Universidad Estatal de Milagro.
- Determinar las amenazas humanas, lógicas y físicas de la infraestructura tecnológica de la Universidad Estatal de Milagro.

1.4. Alcance

El uso de las tecnologías de la información y la comunicación, así como las grandes cantidades de información que se maneja dentro de la institución, conlleva una cantidad de riesgos y amenazas que obligan a tomar acciones para preservar su integridad. Por tal motivo, es importante evaluar las amenazas y los riesgos con el fin de mejorar la seguridad informática de la infraestructura tecnológica de la universidad.

La seguridad informática es la encargada del desarrollo e implementación de los mecanismos de protección informática y de la infraestructura tecnológica, en la actualidad los ataques informáticos han incrementado de tal forma que se han convertido en el pan de cada día de los hackers, debido al crecimiento que ha tenido la tecnología en los últimos tiempos, desencadenado por la nueva era digital y la globalización han permitido que el tema de seguridad informática tome una evolución sin precedentes en los sistemas educativos y en otras áreas (Cando Segovia & Medina Chicaiza, 2021).

A través de este estudio se podrán identificar las amenazas humanas, lógicas y físicas que pueden atacar la infraestructura tecnológica de la universidad, y así estar alerta y contar con las herramientas necesarias para controlar y contrarrestar estos riesgos y amenazas a la seguridad informática. El presente trabajo brinda un beneficio a toda la comunidad universitaria, ya que, con un estudio adecuado se puede brindar una mejor calidad de la información y en especial que cada uno de estos actores cuenten con un sistema seguro al momento de realizar sus actividades.

Al evaluar los riesgos y amenazas que puede sufrir la estructura tecnológica de la institución, se evita en gran medida daños y vulnerabilidades a cualquier tipo de información, como es el caso de las clases virtuales, donde, en la actualidad todo se maneja de forma online, como: las clases de profesor – alumno en las herramientas pertinentes, envíos y recepción de tareas, toma de exámenes, entregas de certificados de cursos o títulos. Por ende, para solventar estas actividades se debe contar con una infraestructura segura capaz de responder a las necesidades, donde no se vea vulnerada la veracidad de la información, es decir que no se pueda violar el sistema. Por lo que es

importante llevar un control y evaluación de riesgos que puede tener la infraestructura tecnológica.

Toda organización independientemente de su dedicación está compuesta por un conjunto de procesos sinérgicos que se comunican entre sí, a través del intercambio de la información transformada, que da completitud, disponibilidad, integridad y calidad del cual depende el éxito de cualquier operación (Santiago & Sanchez, 2017). Por ello se puede considerar que la información es el activo más importante en la actualidad en especial en el sector educativo, donde la mayoría de los procesos se llevan a cabo en forma virtual, con el presente trabajo se busca solucionar problemas de posibles robos de información, ataques en los sistemas y así poder salvaguardar la integridad de los datos de los usuarios que forman parte de la infraestructura tecnológica de la Universidad Estatal de Milagro.

Muchas de las instituciones educativas como en el caso de la Universidad Estatal de Milagro, buscan seguir mejorando e innovando, para brindar una educación de calidad y ofrecer servicios de calidad a todos los que conforman la institución. Mucho más en un mundo tan cambiante como el actual, el tema de seguridad de la información es primordial no solamente en el sector educativo, también en los sectores empresariales, donde la información es un activo indispensable para seguir laborando, por ello se invierte mucho en la seguridad de la información, de la misma manera el sector educativo (Reyes Guerrero, 2017).

El análisis y evaluación de riesgos, la verificación de la existencia de controles de seguridad existentes, las pruebas con software y el monitoreo de los sistemas de información permiten establecer el estado actual de la organización, identificar las causas de vulnerabilidades y proponer soluciones de control que permitan su mitigación (Solarte, Enriquez, & Benavides, 2015). Por lo que los resultados obtenidos en esta investigación servirán de base para un futuro diseño, implementación e implantación de un Sistema de Gestión de Seguridad de la Información - SGSI basado en la Norma ISO/IEC 27001 que permita controlar las vulnerabilidades, amenazas y los riesgos de seguridad a que se ve expuesta la institución.

1.5. Estado del Arte

1.5.1. Antecedente de la investigación

En este trabajo de investigación se utiliza un mapeo sistémico donde se analiza los trabajos que han sido publicados en el buscador de Google Académico. El objetivo propuesto es identificar los trabajos donde describan la evaluación de la seguridad informática o plan de evaluaciones informáticas.

El Sistema de Gestión de la Seguridad Informática SGSI posee la conformación de una estrategia de cómo tratar los aspectos de la seguridad e implica las observaciones necesarias para garantizar el cumplimiento a partir de un análisis de riesgos.

Procesos de un Sistema de Gestión de la Seguridad Informática

El SGSI se compone de cuatro procesos básicos:

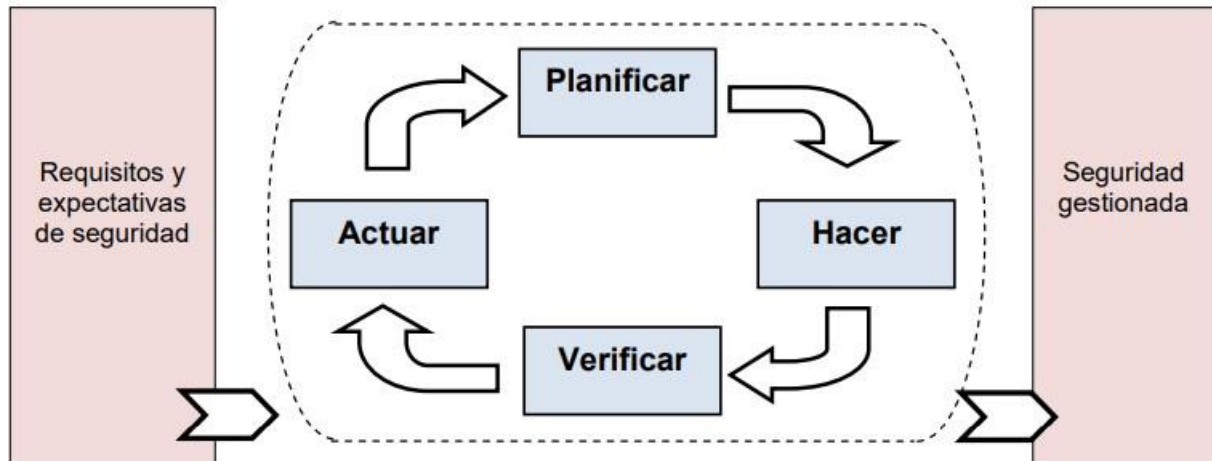


Figura 2. Procesos de un SGSI

1.5.2. Teoría de Sistema

El concepto de Sistemas es múltiple, para poder comprenderlo se debe conocer algunas características de los sistemas: propósitos, globalismo, entropía y homeostasis, así como de los tipos de sistemas posibles y de sus parámetros: entrada, proceso, salida, retroalimentación y ambiente. Dentro de los sistemas el abierto permite hacer un análisis amplio y profundo de las organizaciones.

Las organizaciones se consideran sistemas abiertos, pues su comportamiento es probabilístico y no determinista. Ellas forman parte de una sociedad mayor y están constituidas por partes menores que guardan una interdependencia entre sí. La organización necesita alcanzar la homeostasis o estado de equilibrio. Las organizaciones tienen fronteras o límites más o menos definidos, formulan objetivos y se caracterizan por la morfogénesis.

Al hacer una evaluación crítica de la teoría de sistemas, se evidencia que ese enfoque trajo una gran ampliación en la visión de los problemas organizacionales en contraposición al antiguo enfoque de sistema cerrado. Su carácter integrador y abstracto y la posibilidad de comprensión de los efectos sinérgicos de la organización son realmente sorprendentes. La visión de hombre funcional dentro de las organizaciones es la consecuencia principal de la concepción de la naturaleza humana.

Los objetivos originales de la Teoría General de Sistemas son los siguientes (Bertalanffy, 1976):

- a. Impulsar el desarrollo de una terminología general que permita describir las características, funciones y comportamientos sistémicos.

- b. Desarrollar un conjunto de leyes aplicables a todos estos comportamientos y, por último,
- c. Promover una formalización (matemática) de estas leyes.

La primera formulación en tal sentido se le atribuye al biólogo Ludwig von Bertalanffy, quien acuñó la denominación “Teoría General de Sistemas” (TGS). Para él, la TGS debería constituirse en un mecanismo de integración entre las ciencias naturales y sociales y ser al mismo tiempo un instrumento básico para la formación y preparación de científicos. Sobre estas bases se constituyó en 1954 la Society for General Systems Research, cuyos objetivos fueron los siguientes: (a) Investigar el isomorfismo de conceptos, leyes y modelos en varios campos y facilitar las transferencias entre aquellos; (b) Promoción y desarrollo de modelos teóricos en campos que carecen de ellos; (c) Reducir la duplicación de los esfuerzos teóricos; y (d) Promover la unidad de la ciencia a través de principios conceptuales y metodológicos unificadores (Arnold & Osorio, 1998).

Si bien el campo de aplicaciones de la TGS no reconoce limitaciones, al usarla en fenómenos humanos, sociales y culturales se advierte que sus raíces están en el área de los sistemas naturales (organismos) y en el de los sistemas artificiales (máquinas). Mientras más equivalencias reconozcamos entre organismos, máquinas, hombres y formas de organización social, mayores serán las posibilidades para aplicar correctamente el enfoque de la TGS, pero mientras más experimentemos los atributos que caracterizan lo humano, lo social y lo cultural y sus correspondientes sistemas, quedarán en evidencia sus inadecuaciones y deficiencias (Arnold & Osorio, 1998). Para (Euroinnova, 2019), este enfoque sistémico, permitió comprender de mejor forma a las organizaciones como una serie de subsistemas que se relacionan formando un solo unitario; donde cada uno desarrolla una cadena de eventos que parte de una entrada y culmina en salida, lo que ocurre entre las entradas y las salidas es la esencia del subsistema, conociéndose a esto como proceso.

Una definición de este enfoque se trata de un esfuerzo de estudio interdisciplinario que busca hallar las propiedades comunes a entidades llamadas sistemas. Estos se presentan en todos los niveles, pero son objetivos específicos de diversas disciplinas académicas diferentes. La teoría de los sistemas puede ser aplicada en cualquier ámbito de las ciencias sociales. Al ser una teoría que busca generar pensamiento sistemático, esta ha originado conocimiento dentro de la informática llevando a las personas a desarrollar y trabajar en teorías como la de información o la teoría dinámica de sistemas y la cibernética (Euroinnova, 2019).

1.5.3. Sistemas de Información

El ambiente de los sistemas de información que predominó hasta principios de la década de los noventa, previo a la globalización de las telecomunicaciones, las redes mundiales de teleproceso, la Internet, etcétera tuvo como una de sus características más relevantes la de poseer entornos informáticos en los que se operaba de manera aislada o en redes privadas en las cuales, la seguridad impuesta por el acceso físico y algunas simples barreras informáticas bastaban para que la seguridad de la información en ellos contenida estuviese garantizada (Voutssas, 2010).

Los sistemas de información han ido evolucionando desde mediados del siglo pasado hasta la actualidad, tal como se muestra en la Tabla 1. Según Monasterio (2018), los

sistemas de información se han vuelto imprescindibles con el paso de los años ya que aportan demasiadas ventajas competitivas a las organizaciones frente a aquellas que no se encuentran en disposición de uno:

1950 – 1960, los sistemas de información eran muy simples debido a la tecnología de la época, se utilizaban básicamente para el procesamiento de datos, y tenían como principal función facilitar diferentes tipos de tareas como procesar transacciones, mantener registros o llevar la contabilidad.

1960 – 1970, surgen los sistemas de información gerenciales o MSI que tienen la novedad de transformar los datos almacenados en información útil para ayudar en la toma de decisiones.

1970 – 1980, se produce un avance importante con el surgimiento de las computadoras personales o PC lo que facilitó la expansión de los sistemas informáticos a toda la organización. Un nuevo rol de los SI para proporcionar soporte ad-hoc interactivo para el proceso de toma de decisiones a los gerentes sistemas de información gerencial.

1980 – 1990, surgió la conocida como informática departamental, en la que cada departamento se encargaba de comprar el hardware y software necesario para satisfacer sus necesidades. Esto dio lugar a incompatibilidades entre software de diferentes departamentos y surgieron problemas de conectividad.

1990 – 2000, el surgimiento de Internet cambió drásticamente las capacidades de los sistemas de información ya que hizo posible intercambiar información en tiempo real con diferentes partes del mundo.

2000 – actual, en los últimos años los SI mantienen las funcionalidades que ofrecían anteriormente, sin embargo, han ido mejorando debido a los avances tecnológicos (mayor capacidad de almacenamiento, mejor infraestructura de red, cloud computing etc.). Existe una gran infraestructura de red, un mayor nivel de integración de funciones en todas las aplicaciones y potentes máquinas con mayor capacidad de almacenamiento.

Tabla 1. Evolución de la función de los sistemas de información.

| 1950 – 1960 | 1960 - 1970 | 1970 - 1980 | 1980 - 1990 | 1990 - 2000 |
|---|---|--|---|---|
| Procesamiento de datos | Informes de gestión | Apoyo a las decisiones | Apoyo Ejecutivo | Conocimiento administrativo |
| Recopila, almacena, modifica y recupera transacciones cotidianas de una organización Ayuda a los trabajadores | Informes y pantallas pre especificados para apoyar la toma de decisiones empresariales Ayuda a los gerentes intermedios | Soporte ad-hoc interactivo para el proceso de toma de decisiones Ayuda a los gerentes senior | Proporcione información interna y externa relevante para los objetivos estratégicos de la organización Ayuda a los ejecutivos | Apoya la creación, organización y diseminación del conocimiento empresarial Ayuda disponible para toda la empresa |

Fuente: Tecnologias-informacion.com (2018)

En la actualidad, los sistemas de información han sido sustituidos casi en su totalidad por Las TIC convergentes, por complejas redes institucionales locales y regionales, por

servidores y computadoras personales que cada vez tienen mayor capacidad de proceso y de acceso a otros computadores, y cuya interconexión se extiende mundialmente. Al mismo tiempo, la Internet forma ya parte de la infraestructura operativa de sectores estratégicos de todos los países, y es un factor cada vez más creciente de intercambio de información por parte de los ciudadanos toda vez que se forman redes sociales cada vez más complejas (Voutssas, 2010).

La infraestructura tecnológica ha cambiado sustancialmente, por lo que la cantidad de información ha aumentado significativamente, siendo actualmente un activo muy valioso para casi todas las organizaciones. Por lo tanto, la capacidad de administrar eficientemente esa información influye directamente en la credibilidad, competitividad e imagen de la mayoría de las organizaciones.

De acuerdo con Voutssas (2010), la información se enfrenta a riesgos de daño o pérdida, por sus condiciones de ser digital, multi accesible y necesariamente operada en red. Como resultado de esa creciente interconexión masiva y global, los sistemas y las redes de información se han vuelto más vulnerables, surgiendo nuevos retos que deben abordarse en materia de seguridad. La seguridad informática pretende eliminar o contener estos daños o pérdidas.

1.5.4. Seguridad Informática

Hoy día la seguridad informática es un tema central para todos los usuarios de equipos de cómputo de escritorio o móviles, en el hogar, en la escuela o dentro de una organización, debido a que el uso del Internet con su popularización ha traído consigo importantes riesgos de seguridad (Roque & Juárez, 2018).

De acuerdo con Calvo y otros (2013), la seguridad informática es reconocida como el proceso que vela por la protección de los activos de información, es decir, se establece en el nivel operativo del negocio, pues su fin es brindar soporte al negocio mediante el establecimiento de los controles o buenas prácticas de configuración y el manejo o uso de los diferentes dispositivos que conforman la infraestructura de TI.

La seguridad informática está relacionada con las metodologías, procesos y procedimientos para mantener salvaguardada la información y los datos confidenciales de una organización, al interior de los sistemas informáticos. Los procesos se estructuran con el uso de estándares, normas, protocolos y metodologías para mitigar y minimizar los riesgos asociados a la infraestructura tecnológica (Solarte, Enriquez, & Benavides, 2015).

De acuerdo con Sánchez (2018) la seguridad informática se describe como la distinción táctica y operacional de la seguridad, es decir, las medidas técnicas que aseguran la seguridad de la información. Enfocándose en la protección de infraestructura: redes, sistemas operativos, ordenadores.

El objetivo primario de la seguridad informática es el de mantener al mínimo los riesgos sobre los recursos informáticos, y garantizar así la continuidad de las operaciones de la organización al tiempo que se administra el riesgo informático a un cierto costo aceptable. El objetivo secundario de la seguridad consiste en garantizar que los documentos, registros y archivos informáticos de la organización mantengan siempre su total confiabilidad (Quiroz Zambrano & Macías Valencia, 2017).

La seguridad informática, de igual manera a como sucede con la seguridad aplicada a

otros entornos, trata de minimizar los riesgos asociados al acceso y utilización de determinados sistemas de forma no autorizada y en general malintencionada. El objetivo de la seguridad informática es proteger los recursos informáticos valiosos de la organización, tales como información, hardware o software. A través de la adopción de las medidas adecuadas, la seguridad informática ayuda a una organización a cumplir sus objetivos, permite proteger los recursos financieros, sistemas de información, reputación, situación legal, y otros bienes tanto tangibles e intangible (Galdámez, 2003).

A este respecto se han realizado diversas investigaciones sobre la seguridad informática en la infraestructura tecnológica, considerando elementos como auditorías de seguridad informática, modelos para la gestión de la seguridad informática, seguridad en aplicaciones web, así como concientización y capacitación para incrementar la seguridad informática. A continuación, se presentan antecedentes sobre estudios que aportan referencias teóricas y metodológicas a los investigadores, que son pertinentes a la variable bajo estudio.

Rodríguez (2020), realizó una investigación de tipo documental con el objetivo de describir algunas de las herramientas seleccionadas para el escaneo y explotación de vulnerabilidades, y conceptos fundamentales sobre el hacking ético, teniendo en cuenta las herramientas que se adecuaran a las características de las redes cubanas. Las herramientas expuestas en este trabajo son las más usadas por los especialistas de seguridad tecnológica para detectar, prevenir y responder ante cualquier ataque que se detecte y que afecte la seguridad de las redes: Nmap, Owasp, Metasploit, Bettercap, Armitage, Openvas.

Parada, Florez y Gómez (2018) desarrollaron una investigación sobre los componentes de seguridad desde una perspectiva de la dinámica de los sistemas, como parte de un proyecto de investigación Análisis Sistemático de los Observatorios de Ciberseguridad, con el apoyo de la Universidad Pontificia Bolivariana de Bucaramanga. Realizaron una revisión del estado del arte en función de la Ciberseguridad y la Dinámica de los Sistemas, esto para poder identificar y describir varios elementos que caracterizan a la Ciberseguridad basado en los framework, normas o estándares internacionales como: la Organización Internacional de Estándares (ISO), la Unión Internacional de Telecomunicaciones (ITU), la Agencia Europea de Seguridad de la Información y de las Redes (ENISA).

Roque y Juárez (2018), realizaron una investigación donde buscaban explorar las deficiencias en seguridad informática que poseen los alumnos universitarios de licenciatura en informática de los primeros semestres, hicieron una evaluación preliminar para buscar qué efectos tendría un programa de capacitación y concientización. Trabajaron con un grupo de estudiantes, a quienes se les aplicó una encuesta antes y después de un evento formativo en modalidad de conferencia. Analizaron los datos con SPSS, y realizaron pruebas no paramétricas de Wilcoxon para buscar diferencias entre las respuestas obtenidas antes y después del evento. Se evidenció que los estudiantes podrían tener mayores niveles de conocimientos y seguridad en sus actividades cotidianas de cómputo, logrando incrementar indicadores tales como la percepción de conocimientos de seguridad informática y la conciencia de realizar respaldos más frecuentes.

1.5.5. Infraestructura Tecnológica

Es el equipamiento y conectividad de una organización que permite el soporte o la sustentación de las operaciones de la misma, al referirse a la infraestructura tecnológica dentro de las instituciones educativas, (Muñoz, 2017) la define como: “Conjunto de hardware y software sobre el que se asientan los diferentes servicios que la institución necesita tener en funcionamiento para poder llevar a cabo toda su actividad, tanto docente como de investigación, administración o gestión interna” (pág. 23).

La infraestructura tecnológica cuenta con elementos necesarios para que una institución opere tecnológicamente de manera eficiente y eficaz, además del hardware y software mencionados en el párrafo anterior, (Laudon, 2012) destaca otros componentes como: plataformas de internet, plataformas de sistema operativo, redes/ Telecomunicaciones, consultores e integradores de sistemas y gestión de almacenamiento de datos. El hardware son los componentes físicos que posee el ordenador los cuales pueden ser dispositivos internos o externos (Marcillo, 2021).

- Software por su parte es la contraposición a los componentes físicos, pues es el equipamiento intangible y lógico de los sistemas informáticos (Maida & Pacienza, 2015)
- Plataformas de internet son un conjunto de servidores que permiten llevar a cabo operaciones en internet (Laudon, 2012).
- Al hablar de las plataformas del sistema operativo se hace referencia al “Intermediario entre, por un lado, los programas de aplicación, las herramientas y los usuarios, y, por otro, el hardware del computador” (Stallings, 2012).
- Las redes/telecomunicaciones son un conjunto de elementos que se encuentran interconectados entre sí y hacia el exterior por lo cual se facilita la transmisión de diferentes tipos de información de un usuario a otro.
- Consultores e integradores de sistemas busca integrar los sistemas heredados de una institución a la infraestructura tecnológica contemporánea.
- Debido al aumento de información digital se requiere de un software responsable de gestionar la información de la empresa siendo posible poder acceder a ella de manera eficiente, este almacenamiento puede ser DAS, NAS o SAN (Vázquez, 2015).

Este ecosistema de elementos es fundamental al momento de asegurar un correcto funcionamiento de las instituciones dado que permitirán el almacenamiento, procesamiento y análisis de datos, a la vez que optimizan la productividad y la seguridad de la información.

1.5.6. Estándar ISO/IEC 27001

Las normas ISO 27000 fueron desarrolladas en el año 1995 con la BS 7799 por el Departamento de Comercio e Industria del Reino Unido, estas normas también son conocidas con el nombre “ISO/ IEC” debido a que son desarrolladas y mantenidas por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional, las cuales son organismos internacionales de normalización. El conjunto de normas se

creó a partir de la necesidad de poder contar una base practica de gestión de la seguridad de la información que especifique los requisitos que permitan establecer, implementar, mantener e innovar un SGSI. (Villacis, 2016)

Actualmente existen 45 publicaciones relacionadas a las normas ISO 27000, entre las cuales encontramos la norma 27001, esta norma tiene su origen en la BS 7799-2, es el estándar principal de la serie y se constituye como una norma internacional de certificación para los Sistemas de Gestión de la Seguridad de la Información (Bermeo, 2021)

Esta norma nos brinda un marco robusto para proteger la información sensible que se maneja dentro de una organización, para Kosutic (como se citó en (Ochoa, 2016) la estructura de la norma consiste en investigar y evaluar los riesgos para poder aplicar un tratamiento sistemático a los mismos. Por ello en la actualidad las organizaciones prefieren utilizar un SGSI que cumpla con la norma ISO 27001 debido a que estas ayudan a realizar una evaluación regular para el control y mejora de procesos, proporciona credibilidad al sistema, reduce los riesgos e incertidumbre y ayuda a aumentar las oportunidades de negocio, pues desde la perspectiva de Bermeo (2021) estas normas permiten la: “Protección de los activos, datos financieros, información de los empleados y datos intelectuales” (pág. 18).

La ISO 27001 trabaja bajo el ciclo Deming el cual es un sistema de mejora continua que busca optimizar las actividades empresariales mediante el uso de cuatro etapas que nos permitirán evaluar procesos una y otra vez para de esta manera asegurarnos del progreso continuo de la organización, estas etapas son:

- **Planificación:** proceso en el cual se establecen objetivos, recursos, requisitos del cliente y accionistas, política organizativa e identificar riesgos y oportunidades.
- **Hacer:** en este proceso se implementa toda la planificación.
- **Verificación:** etapa en la cual se controlan y miden los procesos para establecer el rendimiento de la política, objetivos, requisitos y actividades planificadas e informar de los resultados.
- **Actuar:** fase en la cual se toman acciones para mejorar el rendimiento, en la medida de lo necesario.

La última versión de la ISO 27001 es la ISO/IEC 27001:2013 cuenta con 114 objetivos de control, diecinueve objetivos menos a diferencia de la versión del 2005, en esta se da a las organizaciones la plena libertad de poder definir el patrón para establecer la mejora continua que deseen utilizar para la implementación del SGSI (Quille, 2016).

Lograr la certificación ISO 27001 al implantar un SGSI es un gran reto para la mayoría de las organizaciones, pero si este se logra de manera efectiva, se podrán obtener beneficios significativos para las siguientes áreas:

- **Área comercial:** en esta área nos ayuda a aumentar las oportunidades de negocio, dado que permite efectuar los requerimientos legales, una organización superior y brinda apoyo para conseguir una ventaja comercial (Ochoa, 2016).

- **Área operacional:** en esta área nos brinda un enfoque coherente para tener controles robustos en el manejo de amenazas.

Si bien es cierto, las normas ISO 27001 son perfectamente válidas en cualquier organización indistintamente de su tamaño, resulta ser muy necesaria en tres sectores es específico: salud, financiero y público, en este último sector es fundamental dado que permitirá poner en marcha distintos sistemas y protocolos que puedan garantizar la confidencialidad y gestión adecuada de la gran cantidad de datos que se manejan, entre los cuales la mayoría son de carácter personal y cuentan con un alto nivel de criticidad.

Esta norma requiere de una extensa carpeta de documentación, entre aquellos se encuentran el alcance del SGSI, las políticas de seguridad de la información, declaración de aplicabilidad, plan de tratamiento de riesgos, informe de evaluación de riesgos, definición de roles y responsabilidad de seguridad, inventario de activos, procedimiento operativo para gestión de TI, entre otros documentos necesarios para cumplir con la norma ISO 27001, además de ciertos registros como el registro de habilidades, experiencia y calificaciones, monitoreo y resultado de la medición, entre otros (Bermeo, 2021).

CAPÍTULO 2

2. METODOLOGÍA

2.1 Infraestructura de red y componentes de hardware

Mediante la investigación desarrollada dentro de las instalaciones de TIC, se afirma que la infraestructura tecnológica de la red comprende los siguientes de componentes de hardware.

Dentro de la Universidad Estatal de Milagro se cuenta con una gran infraestructura de red soportada por dos proveedores de internet, contando con un enlace principal de fibra óptica y un enlace secundario proveniente del segundo proveedor de internet este haciendo la función de backup, dando una alta disponibilidad de acceso a internet a la institución. Tal como se muestra en la siguiente ilustración. Figura 2. Proveedores de la red UNEMI.

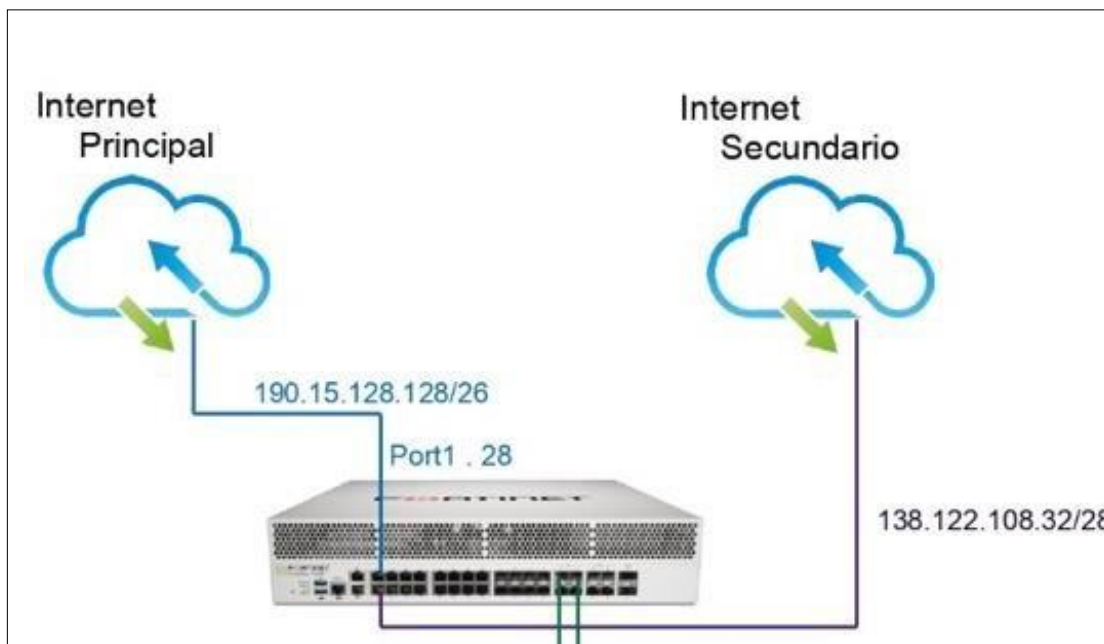


Figura 3. Proveedores de la red UNEMI.
Fuente: Autoría Propia

Estos enlaces se conectan a un router cisco Fortinet, para el debido manejo del tráfico de la red y a su vez la administración del firewall de la institución, tal como se muestra en la Figura 3.

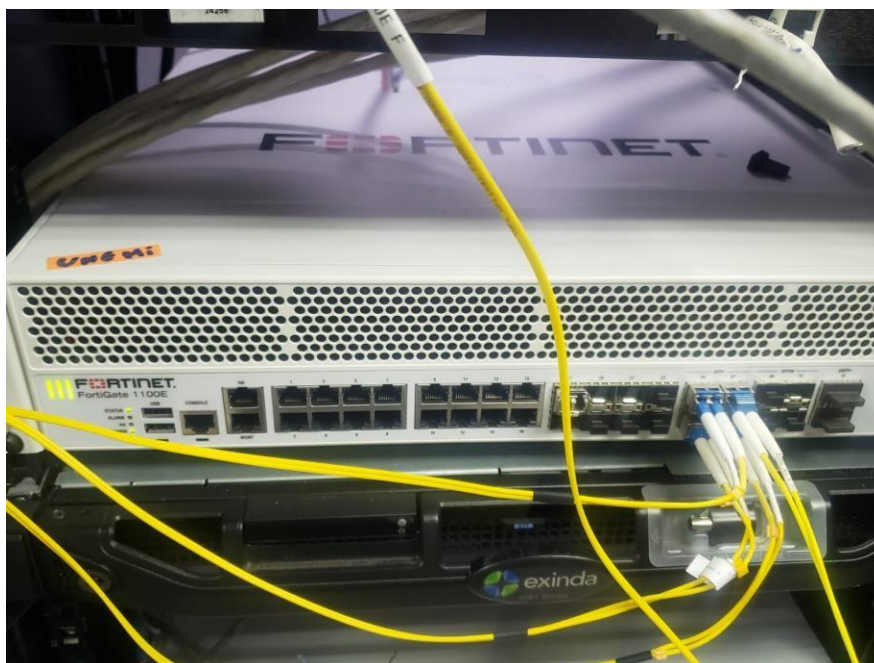


Figura 4. Router Fortinet Cisco.
Fuente: Autoría Propia

Dicho router se conecta a un switch principal a través de patch core y este a una red LAN

de topología estrella donde se conectan cada switch de los diferentes bloques de la universidad. Su función principal es repartir los diferentes enlaces de fibra a los distintos edificios tanto las garitas de acceso, bloques administrativos y los diversos bloques de las aulas de clases. Así como se muestra en la Figura 4.



Figura 5. Switch principal.
Fuente: Autoría Propia

Además del antes mencionado switch se conecta a un servidor DHCP y su respectivo backup para proceder hacer la labor de asignación de ip tanto para los diferentes access point o comúnmente llamados antenas de wifi o puntos de red en los diversos edificios, bloques o aulas. En la siguiente Figura se puede visualizar el servidor DHCP.



Figura 6. Servidor DHCP.
Fuente: Autoría Propia

Y por último el usuario final, tanto estudiante, docente, administrativo etc. Se conectan a la red de la universidad, esto puede ser tanto por cable de red o por wifi.



Figura 7. Antena wifi.
Fuente: Autoría Propia

Estos son los componentes de hardware más relevantes que hacen posible la arquitectura y esquema de toda la red universitaria, la cual soporta la conexión de más de 70.000 estudiantes, docentes y administrativos.

A continuación, se muestra en la Figura 8 el esquema de la arquitectura de red de la Universidad Estatal de Milagro donde se puede visualizar una red redundante en base a un router que permite obtener la conexión de a internet, conectado a un switch core, pasando por los servidores, proveyendo acceso a internet a todos los ordenadores de la institución.

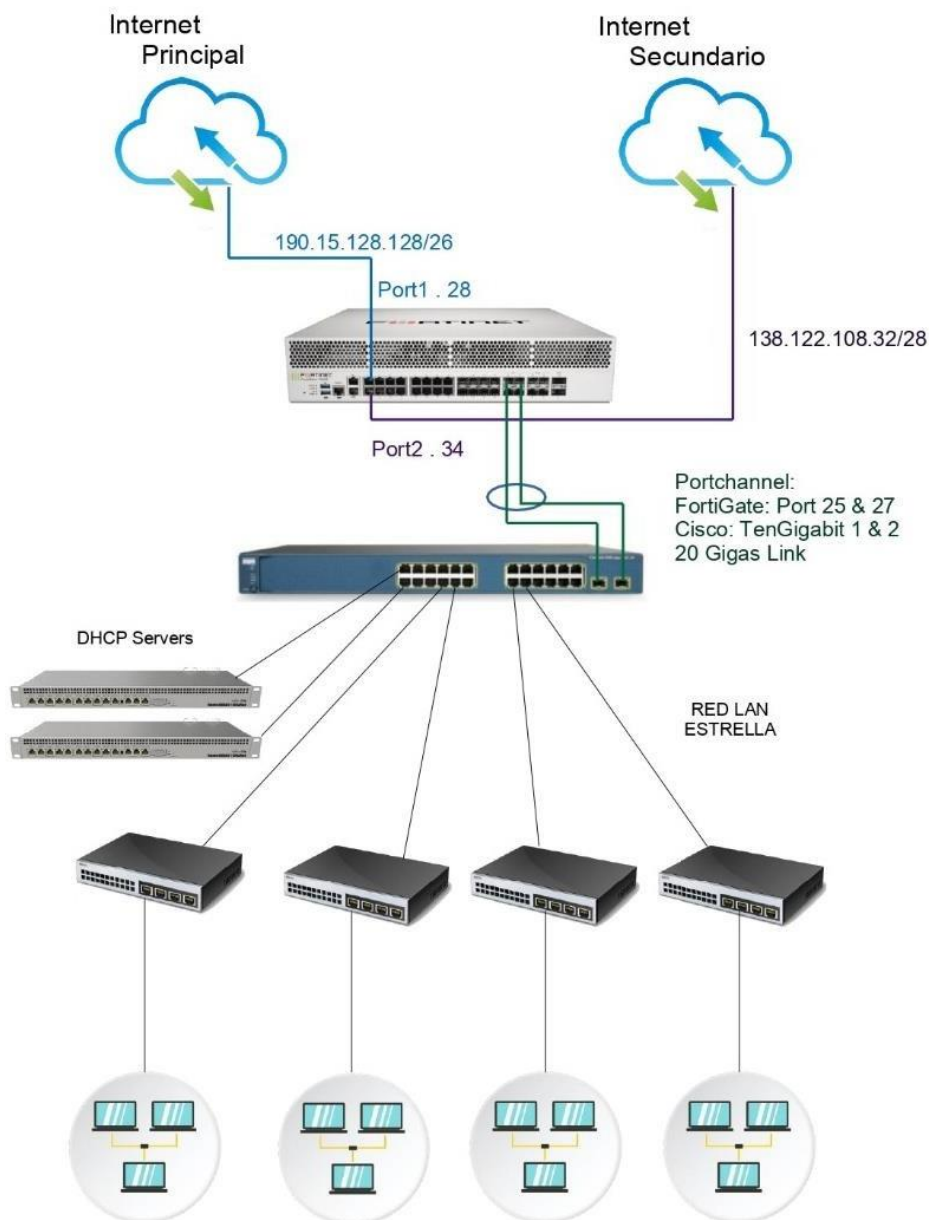


Figura 8. Esquema de infraestructura de red de la red UNEMI.
Fuente: Autoría Propia

2.2 Infraestructura de red y componentes de software

El ataque de cibernautas al sector educativo es bastante frecuente hoy en día. En la actualidad existen muchos casos de universidades que han sufrido ataques incluso de sus propios estudiantes, utilizando software registrador de teclas, también llamados key loggers cuya función es capturar las contraseñas de docentes para poder acceder al

sistema, entre otros a lo largo del tiempo se ha producido innumerables ataques a las universidades de educación superior como los son:

- ✓ Ataques a través de un servidor FTP sin protección.
- ✓ Robo y extorción de la data de empleados y alumnos.
- ✓ Captura de la página web principal de la institución,

Las instituciones de educación superior contienen grandes cantidades de datos sensibles, incluyendo los datos financieros, estadísticos de investigación costosa. Lo que los hace blanco directo para hackers en todo el mundo (auditoriainterna.usta.edu.co, 2022). Por tal motivo es fundamental un monitoreo de la red, usando herramientas o software para dichos monitoreos.

Dentro de una institución educativa es de suma importancia el uso de herramientas o software para detección o prevención de ataques maliciosos, así como el monitoreo constante de ciertos componentes de red. Según el análisis e investigación que se hizo en el departamento de tics, existen los siguientes softwares o herramientas de monitoreo.

Una de las herramientas de vital importancia dentro de una infraestructura tecnológica es el firewall, el encargado de administrar toda la red universitaria en este caso. Su principal función recae en la creación de redes seguras, dando una protección amplia y automatizada contra amenazas sofisticadas y emergentes. Entre las principales características con la que cuenta este dispositivo es el control de aplicaciones, antivirus, sandboxing, inspección de SSL, prevención de intrusos. En la Figura 9 se visualiza una pequeña ventana del software del firewall Fortinet implementado en la red UNEMI.

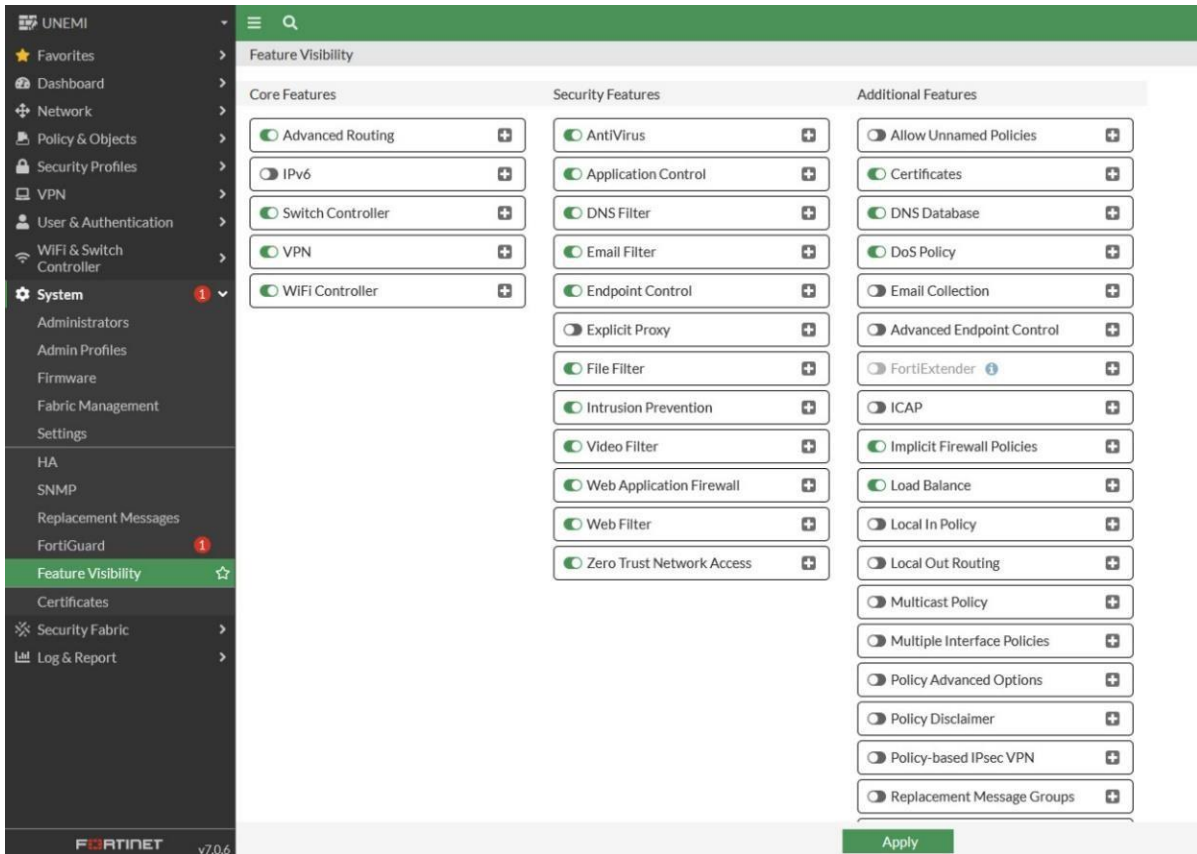


Figura 9. Firewall Fortinet UNEMI.
Fuente: Autoría Propia

Otra de las herramientas de suma importancia para el monitoreo y la alta respuesta ante la eventualidad de la red, es el software de control de las AP (access point) o antenas wifi. Dado que una universidad de educación superior cuenta con muchas aulas y la importancia de la conexión a internet es de carácter vital para cada sesión de clase.

En la Figura 10 se puede visualizar el monitoreo de cada una de las antenas de wifi en los diferentes bloques.

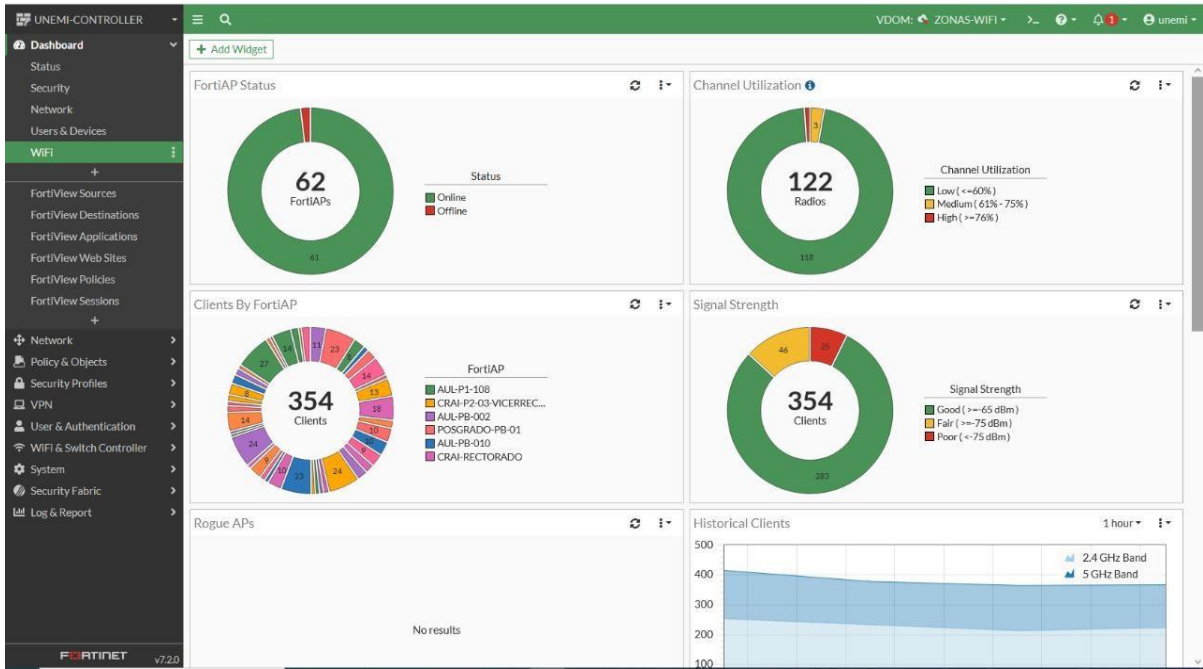


Figura 10. Controladora de antenas wifi UNEMI.
Fuente: Autoría Propia

Si bien en la Figura anterior se puede ver que es una interfaz dedicada para el monitoreo de las antenas wifi de la institución. UNEMI utiliza otra herramienta para el monitoreo de todos los switches que se encuentra en cada uno de los bloques. Esta herramienta es una de libre de distribución llamada ZABBIX, el cual su principal función es verificar que todos los puertos estén conectados, aseverando la correcta conexión de cada bloque. Tal como se muestra en la Figura 11 a continuación.

| Time | Severity | Recovery time | Status | Info | Host | Problem | Duration | Ack | Actions | Tags |
|----------|-------------|---------------|---------|-----------------------|-----------------------|--|------------|-----|---------|------|
| 10:48:07 | Warning | | PROBLEM | Zabbix server | Zabbix server | sda: Disk read/write request responses are too high (read > 20 ms for 15m or write > 20 ms for 15m) | 6h 17m 43s | No | + | - |
| 16:45:11 | Average | | PROBLEM | switch_Carita_Ingreso | switch_Carita_Ingreso | Interface gi1/1/21(): Link down | 20m 39s | No | + | - |
| 12:13:16 | Average | | PROBLEM | switch_J | switch_J | Interface Gi1/0/5(Aula 107 bloque J): Link down | 4h 52m 34s | No | + | - |
| 10:46:16 | Average | | PROBLEM | switch_J | switch_J | Interface Gi1/0/3(Aula 105 bloque J): Link down | 6h 19m 34s | No | + | - |
| 10:08:16 | Average | | PROBLEM | switch_J | switch_J | Interface Gi1/0/2(Aula 104 bloque J): Link down | 6h 57m 34s | No | + | - |
| 13:15:40 | Average | | PROBLEM | switch_CRAI-3P-1 | switch_CRAI-3P-1 | Interface Gi0/41(): Link down | 3h 50m 10s | No | + | - |
| 09:10:38 | Information | | PROBLEM | switch_CRAI-2P-2 | switch_CRAI-2P-2 | Interface Gi0/41(): Ethernet has changed to lower speed than it was before | 7h 55m 12s | No | + | - |
| 16:17:38 | Average | | PROBLEM | switch_CRAI-2P-2 | switch_CRAI-2P-2 | Interface Gi0/32(CUBICULO-17): Link down | 48m 12s | No | + | - |
| 16:19:39 | Average | | PROBLEM | switch_CRAI-3P-1 | switch_CRAI-3P-1 | Interface Gi0/28(CUBICULO-113): Link down | 48m 11s | No | + | - |
| 08:30:37 | Information | | PROBLEM | switch_CRAI-2P-1 | switch_CRAI-2P-1 | Interface Gi0/27(audifonia-externa): Ethernet has changed to lower speed than it was before | 8h 35m 13s | No | + | - |
| 16:50:07 | Information | | PROBLEM | switch_C | switch_C | Interface Gi0/24(BC-P2-PP1-P24 Enlace hacia switch bloque c planta baja): Ethernet has changed to lower speed than it was before | 15m 43s | No | + | - |
| 16:10:12 | Information | | PROBLEM | switch_B | switch_B | Interface Gi0/22(): Ethernet has changed to lower speed than it was before | 55m 38s | No | + | - |
| 12:30:40 | Average | | PROBLEM | switch_CRAI-3P-2 | switch_CRAI-3P-2 | Interface Gi0/21(CUBICULO-72): Link down | 4h 35m 10s | No | + | - |
| 16:12:30 | Average | | PROBLEM | switch_S | switch_S | Interface Gi0/21(): Link down | 53m 20s | No | + | - |
| 16:49:12 | Average | | PROBLEM | switch_B | switch_B | Interface Gi0/20(ARQUITECTO OBRAS UNIVERSITARIAS): Link down | 16m 38s | No | + | - |
| 12:04:39 | Average | | PROBLEM | switch_CRAI-2P-2 | switch_CRAI-2P-2 | Interface Gi0/19(CUBICULO-20): Link down | 5h 1m 11s | No | + | - |
| 15:53:30 | Average | | PROBLEM | switch_S | switch_S | Interface Gi0/19(conexion 1 vmware-hp): Link down | 1h 12m 20s | No | + | - |
| 12:55:30 | Average | | PROBLEM | switch_S | switch_S | Interface Gi0/18(conexion 2 web server): Link down | 4h 10m 20s | No | + | - |
| 16:54:07 | Average | | PROBLEM | switch_C | switch_C | Interface Gi0/18(AP-BC-P2-PP1-P18-SW1-P-18 Antena RRH): Link down | 11m 43s | No | + | - |
| 16:11:30 | Average | | PROBLEM | switch_S | switch_S | Interface Gi0/17(conexion 1 web server): Link down | 54m 20s | No | + | - |
| 16:10:28 | Information | | PROBLEM | switch_R-DataCenter3 | switch_R-DataCenter3 | Interface Gi0/16(IVAN SALTOS): Ethernet has changed to lower speed than it was before | 55m 22s | No | + | - |

Figura 11. Software de monitoreo Zabbix UNEMI.
Fuente: Autoría Propia

Para un administrador de red es sumamente importante disponer de herramientas que permitan realizar su trabajo de forma ordenada, ágil y simple. Si se habla de redes y manejo de ip otra de las herramientas que usa la Universidad Estatal de Milagro UNEMI es PHPIPAM el cual su principal propósito es la gestión de las subredes y además la posibilidad de acceder a ella desde cualquier dispositivo dentro de la red en otras palabras, es un gestor de direcciones ip para evitar el desperdicio de estas en la institución. Tal como se muestra en la Figura 12.

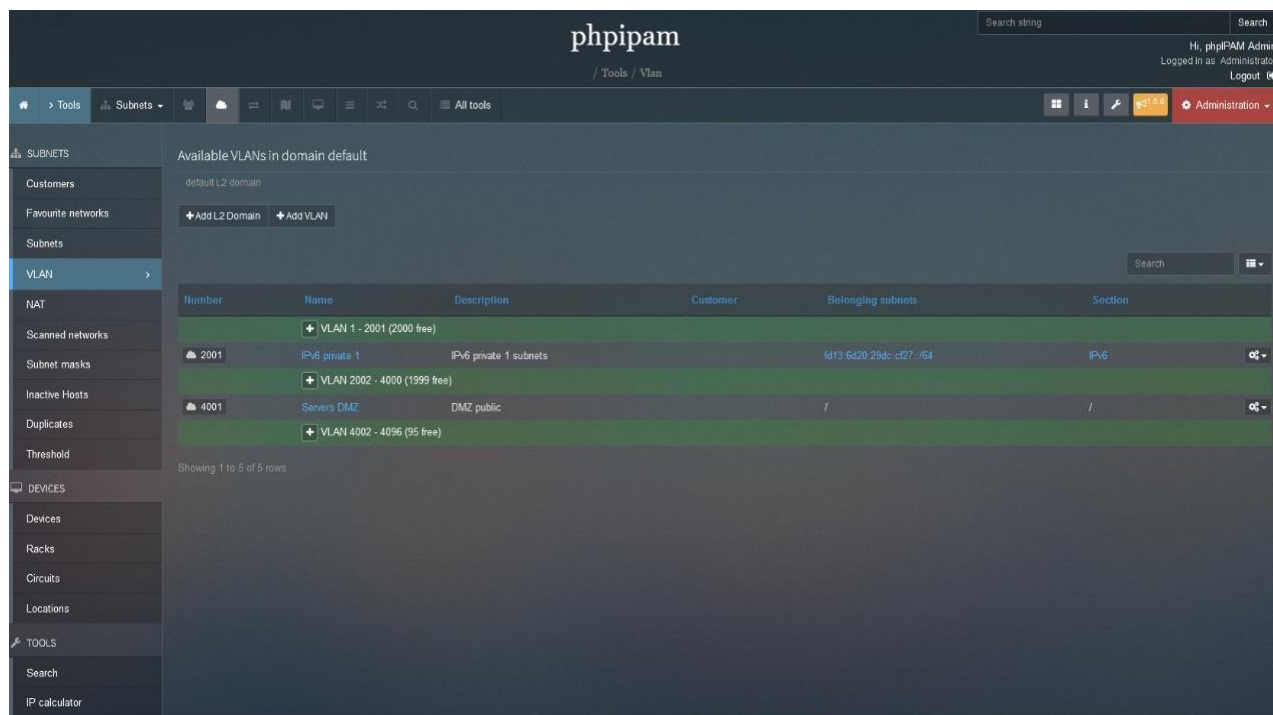


Figura 12. Administrador de direcciones ip PHPIPAM
Fuente: Autoría Propia

2.3 Método de desarrollo

La metodología de desarrollo forma parte del proceso de cualquier proyecto, sistema o producto que se quiere implementar, donde debe describir técnicas y métodos que se ha seguido para lograr los objetivos propuestos, dando un mejor resultado en el tiempo de la entrega final del trabajo.

De los varios tipos de metodologías que se encontraron para la evaluación de la seguridad de la información, se definió el uso de la metodología AMFE (Análisis Modal de Fallos y Efectos). La cual es una metodología que se usa para predecir y estimar los fallos que en un producto puede suceder y se encuentra en fase de diseño, con la finalidad que desde un inicio incorpore todos los componentes, funciones y funcionalidades, donde garantice su fiabilidad, seguridad y cumplimiento de los parámetros que los clientes exijan del nuevo producto.

El AMFE, dentro de la ingeniería de calidad es una de las herramientas más comunes que reduce o previene fallos potenciales durante el desarrollo de productos. Esta herramienta de manera general ha referido un grupo de actividades para:

- Identificar procesos que eliminen o reduzcan las probabilidades de falla.
- Evaluar y reconocer potenciales fallas y sus posibles efectos.
- Documentar o describir la información del análisis.

La aplicación de esta metodología permitió:

- Conocer a fondo el proceso de seguridad informática de la Universidad Estatal de Milagro.
- Identificar las posibles fallas.
- Identificar los efectos.
- Identificar las causas de las posibles fallas.
- Establecer niveles de confiabilidad.
- Evaluar el nivel de criticidad de los efectos.
- Evaluar mediante indicadores específicos la relación: gravedad, ocurrencia y defectibilidad.
- Documentar los planes de acción para minimizar los riesgos.

2.4 Fase para la obtención de evidencia

Para la presente investigación, fue indispensable realizar una solicitud de aprobación para el progreso de la investigación a la Dirección de Tecnologías de la Información y Comunicaciones de la Universidad Estatal de Milagro (UNEMI), con el fin de recolectar información de primera mano que refleje los procesos de seguridad de la red, además de los protocolos con el fin de hacer un diagnóstico de manera minuciosa de la problemática. Se tomó en cuenta realizar encuestas tipo checklist al personal en la Dirección de Tecnologías de la Información y Comunicaciones (TIC) de carácter sensible, permitiendo recabar datos de los distintos problemas de forma dinámica y específica.

Para medir la situación actual con respecto al caso de estudio, se diseñó un esquema basado en la norma ISO 27001 el cual posee 6 componentes a evaluar con sus respectivos ítems, tal como se muestran a continuación en las siguientes Tablas 2, 3, 4, 5, 6, 7.

Tabla 2. Componente Inventario Activo

| Componente | Items |
|-------------------|--|
| Inventario activo | 1. ¿Posee con un Plan Estratégico? |
| | 2. Posee un control de los inventario de los activos en formatos físicos? |
| | 3. Posee un control los inventario de los activos en formatos electrónicos? |
| | 4. ¿Registra un control los inventarios de los activos de soporte de hardware? |
| | 5. ¿Registra un control los inventarios de los activos de soporte de software? |
| | 6. ¿Posee control los inventarios de los activos de soporte de redes? |
| | 7. Registra activos o grupos de activos que no poseen custodios asignados? |

Tabla 3. Componente Seguridad de los Recursos Humanos

| Componente | Items |
|-----------------------------------|---|
| Seguridad de los Recursos Humanos | 1. ¿Se relacionan los procedimientos de mantenimiento correctivo, preventivo de los bienes: Software, Hardware y equipos de comunicación? |
| | 2. ¿Se atribuye o notifica al personal del mal uso y destrucción de los equipos tecnológicos asignados? |
| | 3. ¿El departamento de tecnología tiene restringido con claridad sus responsabilidades? |
| | 4. ¿Se posee objetivos para el departamento de tecnología? |
| | 5. ¿Posee definido por escrito los objetivos del departamento de tecnología? |
| | 6. ¿El personal que trabaja en el departamento de informática son los adecuados para cumplir las necesidades de este? |
| | 7. ¿El departamento tecnológico posee conflictos por la carga de trabajo? |
| | 8. ¿Bajo qué criterios existe la falta de cumplimiento de sus funciones? |
| | 9. ¿Se efectúa la devolución de los equipos tecnológicos del personal que finaliza su contrato de trabajo por escrito? |

Tabla 4. Componente Seguridad Física del Entorno

| Componente | Items |
|------------------------------|--|
| Seguridad Física del Entorno | 1. ¿Se encuentran los repuestos y soportes de los equipos a una distancia prudente para evitar daños en caso de desastre de las instalaciones principales? |
| | 2. ¿Se ubica el equipo apropiado contra incendios? |
| | 3. ¿Se efectúan mantenimientos de las instalaciones eléctricas y ups? |
| | 4. ¿Se efectúan mantenimientos de los sistemas de climatización y ductos de ventilación? |
| | 5. ¿Se establecen controles para minimizar el riesgo de amenazas físicas, tales como robo, incendio, entre otras? |
| | 6. ¿Existen garantías físicas para trabajar en las áreas seguras? |
| | 7. ¿Los equipos se encuentran correctamente ubicados o protegidos de las amenazas o peligros del entorno? |
| | 8. ¿Se da seguimiento de las condiciones ambientales de humedad y temperatura? |
| | 9. ¿Se posee protección contra variaciones de energía o descargas eléctricas en las edificaciones de la institución? |
| | 10. ¿Se posee filtros protectores en las líneas de comunicación y en el suministro de energía? |

| | |
|--|---|
| | 11. ¿Los equipos tecnológicos cuentan con protección contra fallas de suministro de energía? |
| | 12. ¿Se garantiza el cableado de la red contra daño? |
| | 13. ¿Se garantiza el cableado de energía de los cables de red? |
| | 14. ¿Se separan los cables de energía de los cables de red según los estándares para el correcto funcionamiento de la red en el Data Center? |
| | 15. ¿Se establecen las normativas locales e internacionales para la implementación de las redes? |
| | 16. ¿Se dispone de documentación, planos, diseños, de la distribución de todas conexiones de redes alámbricas e inalámbricas? |
| | 17. ¿Se posee un control de mantenimientos periódicos de los dispositivos tecnológicos y los equipos de acuerdo a las especificaciones y recomendaciones del proveedor? |
| | 18. ¿El personal calificado y autorizado realiza los mantenimientos de los equipos tecnológicos? |
| | 19. ¿Se guardan registros de los mantenimientos correctivos, preventivos, fallas relevantes o sospechosas? |
| | 20. ¿Se constituyen controles de mantenimientos programados? |
| | 21. ¿Posee un registro de los mantenimientos correctivos y preventivos? |
| | 22. ¿Posee custodia los equipos y medios que se encuentran fuera de la institución? |
| | 23. ¿Posee cobertura de seguro para proteger los equipos que se encuentran fuera de la institución? |
| | 24. ¿Posee control de acceso para las redes inalámbricas del establecimiento? |
| | 25. ¿Posee control de acceso a los servidores? |
| | 26. ¿Posee un formulario de evaluación a los dispositivos deteriorados que contengan información sensible antes de enviar a reparación? |
| | 27. ¿Posee un manual de borrado para equipos con información sensible o reutilizado? |
| | 28. ¿Posee la autorización necesaria previa para el retiro de cualquier equipo, información o software? |
| | 29. ¿Poseen identificación las personas autorizadas para el retiro de los activos del establecimiento? |
| | 30. ¿Posee un registro del equipo o activo se ha retirado o cuando se ha devuelto? |

Tabla 3. Componente Gestión de Comunicación y de Operación

| Componente | Items |
|--|---|
| Gestión de Comunicación y de Operación | 1. ¿Posee documentación del proceso de respaldo y restauración de la información? |
| | 2. ¿Posee documentación o instrucciones para el manejo de errores y otras condiciones que pueden surgir mediante ejecución de tareas? |
| | 3. ¿Posee documentación de los procedimientos para el reinicio y recuperación del sistema en caso de fallas? |
| | 4. ¿Posee programación del proceso de cambio con su prueba correspondiente? |
| | 5. ¿Se delegan responsables de control de cambios en los equipos tecnológicos y software? |
| | 6. ¿Se autorizan de manera formal los cambios o recomendaciones propuestas? |
| | 7. ¿Posee distribución de responsabilidades y funciones en el Departamento Tecnológico? |
| | 8. ¿Posee gestiones de escalabilidad para asegurar el desempeño requerido de los servicios y sistemas informáticos? |
| | 9. ¿Posee un bloqueo de software no autorizado o ajenos a terceros para la institución? |

| | |
|--|---|
| | 10. ¿Posee instalación y actualización automática de software de antivirus contra código malicioso? |
| | 11. ¿Se posee los sistemas operativos actualizados con las últimas versiones estable? |
| | 12. ¿Posee políticas de respaldo de la información antes del mantenimiento? |
| | 13. ¿Las áreas de redes y mantenimiento se encuentran separadas? |
| | 14. ¿Denominan responsabilidades y procedimientos para la asistencia de equipos remotos? |
| | 15. ¿Hacen diseños, planos antes de la implementación de una red? |
| | 16. ¿Se verifican fallas o alertas del sistema operativo ? |
| | 17. ¿Se efectúan cambios de configuración de seguridad del sistema operativo? |

Tabla 4. Componente Control de Acceso

| Componente | Items |
|------------------------------|---|
| Componente Control de Acceso | 1. ¿Se documenta y encuentran identificados los equipos de las redes? |
| | 2. ¿Posee documentada la identificación de todos los equipos que permitidos de la red? |
| | 3. ¿Se implementan procedimientos para controlar la instalación de software en sistemas operativos? |
| | 4. ¿Posee un registro de las actualizaciones de software que se realizan, tipo auditoria? |
| | 5. ¿El sistema operativo posee restricciones de cambios o instalación de paquetes de software? |
| | 6. ¿Posee documentación del control de versiones para todas las actualizaciones de software? |

Tabla 5. Componente Cumplimiento

| Componente | Items |
|--------------|---|
| Cumplimiento | 1. ¿Se posee inventario de todas las normas legales, estatutos y reglamentos pertinentes para cada programa de software, servicio informático e información que utilice el establecimiento? |
| | 2. ¿Posee conocimiento de las leyes y normas generales relacionadas a la gestión de datos e información electrónica? |

Cada uno de los componentes se calificaron con un checklist usando la escala de Likert por el nivel de información o importancia de la investigación, teniendo en cuenta estos criterios permitiendo determinar los valores de la siguiente forma:

| Escala | Descripción |
|--------|-----------------------|
| 1 | No cumple |
| 2 | Cumple sin evidencias |
| 3 | Cumple a medias |
| 4 | Cumple |

Para una mejor visualización con respecto a calificación visualizar el Anexo 2. Con base a las respuestas y evidencias obtenidas por parte del personal de la Dirección TIC se pudo determinar los resultados de cumplimiento a los estándares ISO 27001 con relación a los procesos.

CAPÍTULO 3

3. EVALUACION, AMENAZAS Y VULNERABILIDADES

Para la respectiva evaluación del proyecto se tuvo en cuenta la metodología descrita anterior con referencia a las normas ISO 27001. Se procedió a hacer encuestas a los principales funcionarios a cargo de la infraestructura y su respectiva dirección donde se pudo obtener datos, los cuales permitieron identificar las vulnerabilidades según el cumplimiento de la norma. Para luego ser analizado y evaluado mediante la metodología AMFE, clasificando por los diferentes dispositivos o componentes principales de la red, para así ponderar el impacto para obtener un nivel de riesgos y así poder tomar acciones de mitigación y aceptación por parte de la Dirección TIC.

Para el desarrollo del objetivo, se realizó una calificación de cada componente según la norma ISO 27001, obteniendo los resultados mostrados en las siguientes Tablas.

La información presentada en la Tabla 8 corresponde a los datos recolectados del componente inventario de activo basado en las normativas ISO 27001 lo cual arrojó como resultado que posee un total de 3 vulnerabilidades que **no cumple** y a su vez 3 vulnerabilidades que **cumple a medias**, representados en un 43%.

Tabla 6. Calificación del componente Inventario Activo según la norma ISO 27001

| Componentes | Criterios | Numero de Vulnerabilidades | Frecuencia |
|----------------------|-----------------------|----------------------------|-------------|
| INVENTARIO DE ACTIVO | No cumple | 7 | 43% |
| | Cumple sin evidencias | 1 | 14% |
| | Cumple a medias | 3 | 43% |
| | Cumple | 0 | 0% |
| Total | | 7 | 100% |

Fuente: Autoría Propia

En la Tabla 9 los datos recolectados del componente de la norma ISO 27001 de seguridad física con respecto al entorno, se evidencia como resultado 21 vulnerabilidades **cumple sin evidencia** representados en un 70%.

Tabla 7. Calificación del componente Seguridad Física según la norma ISO 27001

| Componentes | Criterios | Numero de Vulnerabilidades | Frecuencia |
|--------------------|-----------------------|-----------------------------------|-------------------|
| SEGURIDAD FÍSICA | No cumple | 5 | 17% |
| | Cumple sin evidencias | 21 | 70% |
| | Cumple a medias | 1 | 3% |
| | Cumple | 3 | 10% |
| Total | | 30 | 100% |

Fuente: Autoría Propia

La Tabla 10 corresponde a los datos recolectados del componente de seguridad de los recursos humanos con la norma ISO 27001 dando como resultado 3 vulnerabilidades con criterio **cumple**, 3 vulnerabilidades con criterio **cumplen sin evidencias** y 3 más con criterio **No cumple**, representados en 33% cada uno de ellos.

Tabla 8. Calificación del componente Seguridad de los RRHH según la norma ISO 27001.

| Componentes | Criterios | Numero de Vulnerabilidades | Frecuencia |
|-----------------------------------|-----------------------|-----------------------------------|-------------------|
| SEGURIDAD DE LOS RECURSOS HUMANOS | No cumple | 3 | 33% |
| | Cumple sin evidencias | 3 | 33% |
| | Cumple a medias | 0 | 0% |
| | Cumple | 3 | 33% |
| Total | | 9 | 100% |

Fuente: Autoría Propia

En la Tabla 11 los resultados de los datos de gestión de comunicación y de operación fundamentado en la norma ISO 27001, da como resultado 10 vulnerabilidades **Cumple sin evidencias**, representados en un 59%.

Tabla 9. Calificación del componente gestión de comunicación y operación según la norma ISO 27001.

| Componentes | Criterios | Numero de Vulnerabilidades | Frecuencia |
|-------------------------------------|-----------------------|----------------------------|-------------|
| GESTIÓN DE COMUNICACIÓN Y OPERACIÓN | No cumple | 6 | 35% |
| | Cumple sin evidencias | 10 | 59% |
| | Cumple a medias | 0 | 0% |
| | Cumple | 1 | 6% |
| Total | | 17 | 100% |

Fuente: Autoría Propia

En la tabla 12 se puede visualizar la información que corresponde al componente control de acceso, dieron como resultado un total de 3 de vulnerabilidades del criterio **Cumple sin evidencias** correspondiente al 50%.

Tabla 10. Calificación del componente Control de Acceso según la norma ISO 27001.

| Componentes | Criterios | Numero de Vulnerabilidades | Frecuencia |
|-------------------|-----------------------|----------------------------|-------------|
| CONTROL DE ACCESO | No cumple | 2 | 33% |
| | Cumple sin evidencias | 3 | 50% |
| | Cumple a medias | 0 | 0% |
| | Cumple | 1 | 17% |
| Total | | 6 | 100% |

Fuente: Autoría Propia

En la Tabla 13 la información recolectada corresponde al cumplimiento según la norma ISO 27001, donde se puede evidenciar 2 vulnerabilidades del criterio **no cumple**

Tabla 11. Calificación del componente Cumplimiento según la norma ISO 27001

| Componente | Criterio | Numero de Vulnerabilidades | Frecuencia Relativa |
|--------------|-----------------------|----------------------------|---------------------|
| CUMPLIMIENTO | No cumple | 2 | 75% |
| | Cumple sin evidencias | 1 | 25% |

| | | |
|-----------------|----------|-------------|
| Cumple a medias | 0 | 0% |
| Cumple | 0 | 100% |
| Total | 3 | 100% |

Fuente: Autoría Propia

En la Figura 13 presentada se puede evidenciar el total de 39 vulnerabilidades con criterio **Cumple sin evidencia**. De los cuales el mayor número de vulnerabilidades fueron en el componente seguridad física del entorno, seguida por el componente gestión de comunicación y de operación.

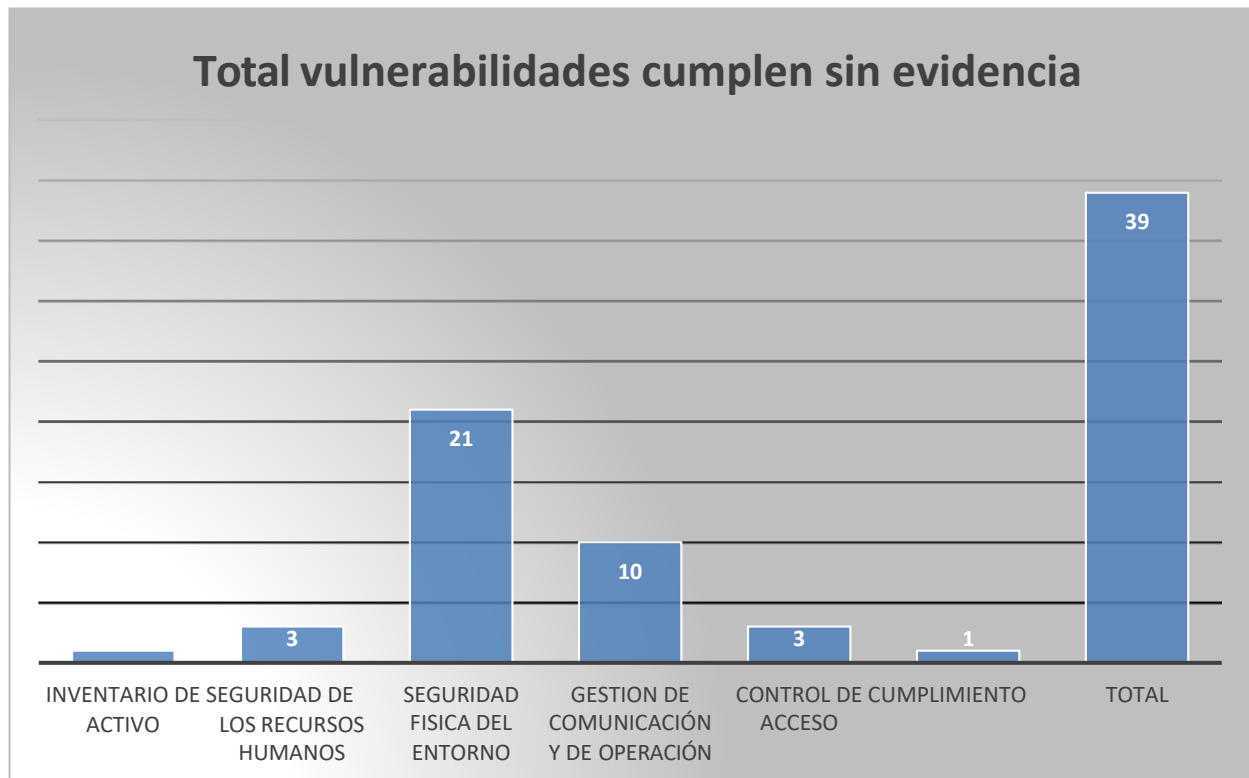


Figura 13. Total de vulnerabilidades

Fuente: Autoría Propia

En la Figura 14 se evidencia un total de 21 de vulnerabilidades encontradas de todos componentes que **no cumple**, los cuales el 29% pertenece al componente Gestión de Comunicación y de Operación, 24% Seguridad Física del Entorno, 14% tanto para Inventario de Activo y Seguridad de recursos Humanos, 10% Cumplimiento y 9% para Control de Acceso.

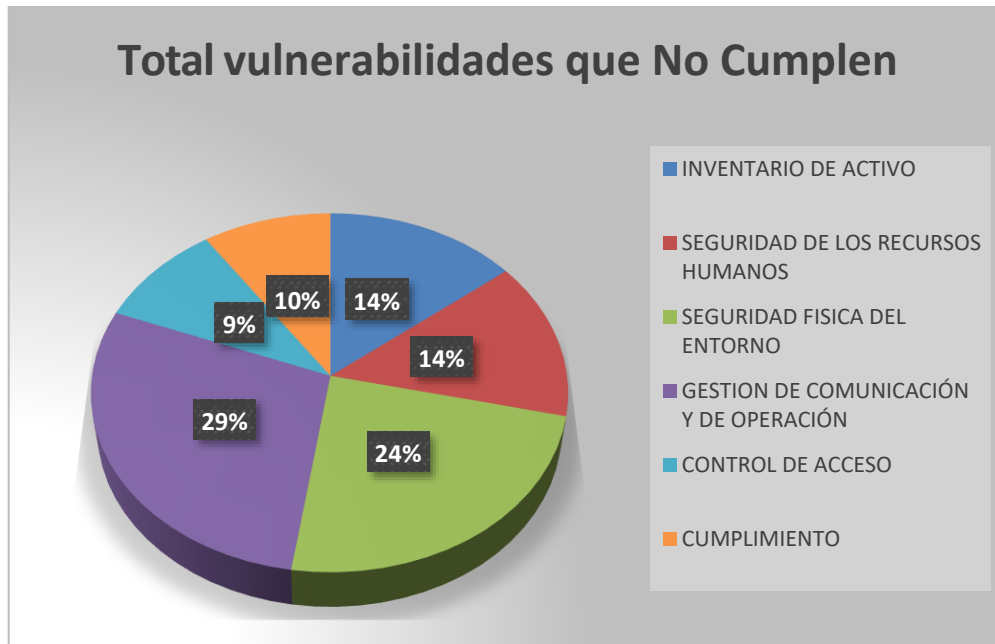


Figura 14 Total de vulnerabilidades que No Cumplen

Fuente: Autoría Propia

Con todo lo antes mencionado se puede evidenciar en la siguiente Figura 15 las vulnerabilidades detectadas de cada componente de acuerdo a la norma ISO 27001. Los datos presentados evidencian una falta de control al cumplimiento de la norma y contar con los respectivos respaldos de la documentación de procesos y manejo eficiente.

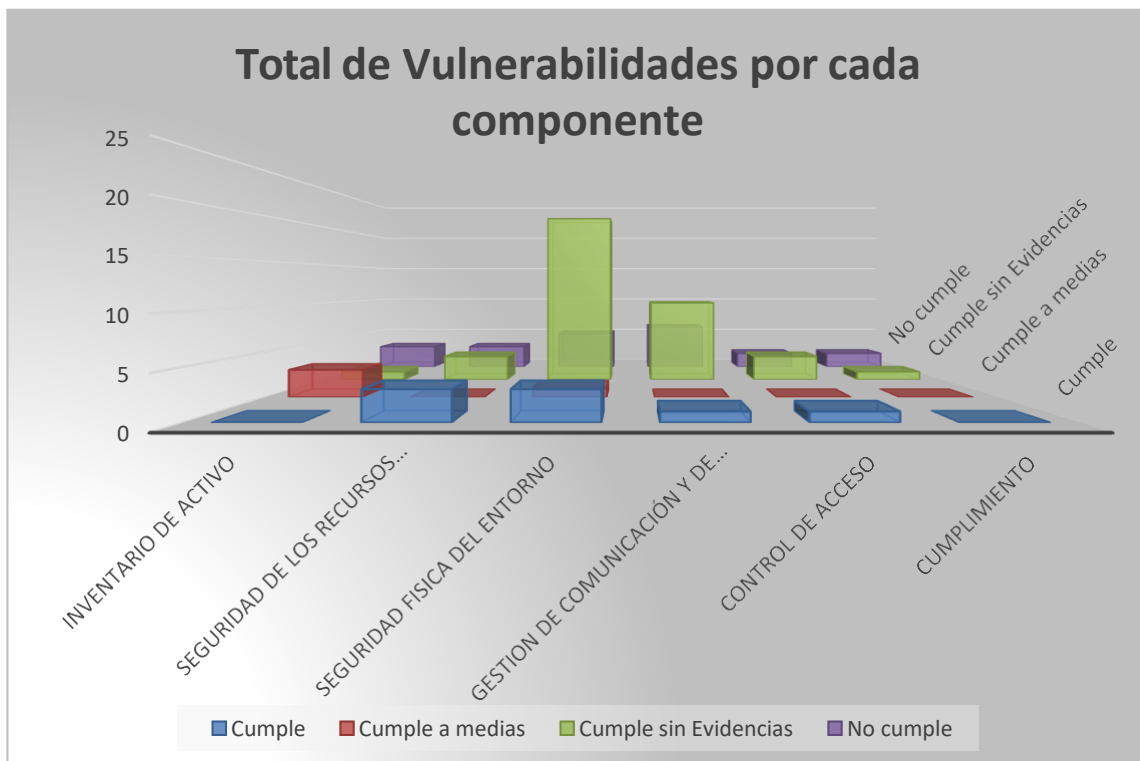


Figura 15 Total de Vulnerabilidades por cada componente

Fuente: Autoría Propia

3.1 Evaluación y Amenazas

Para la realización del objetivo principal de este proyecto, primeramente, se necesitó obtener los resultados de los objetivos anteriores con el cual se puede evidenciar el estado actual de las vulnerabilidades de la Universidad Estatal de Milagro, Tablas 8, 9, 10, 11, 12, 13. Para luego ser analizados y evaluados, clasificando por cada componente las vulnerabilidades y ponderando por impacto, probabilidad el nivel de riesgo, de tal forma se pueda tomar acción de mitigación y criterio de aceptación.

Se obtuvo resultados empleando la matriz de riesgos AMFE, se establecieron para cada una de las vulnerabilidades encontradas en el checklist realizado con la norma ISO 27001 los cuales se encuentran clasificados por cada componente establecida por la norma ISO 27001. Para una mejor comprensión se presenta a continuación en las Tablas 14, 15, 16, 17, 18 y 19 las vulnerabilidades encontradas a través del checklist basado en la Norma ISO/IEC 27001.

Dentro de los aspectos más relevantes, se pudieron evidenciar el alto índice de vulnerabilidades que se cumplen a medias, esto quiere decir que se debe llevar un mejor control del cumplimiento de la norma.

Tabla 12. Vulnerabilidades en el componente Inventario de Activo.

| INVENTARIO DE ACTIVO | | | |
|----------------------|---|-----------------------|---|
| Vulnerabilidades | | | |
| Cumple | Cumple a medias | Cumple sin Evidencias | No cumple |
| | Llevan los inventarios de los hardware que llega | | Se tiene un plan estratégico |
| | Llevan los inventarios de las herramientas para el soporte de red | | Se llevan el inventario de los activos automatizados |
| | Existen muchos activos que no tienen custodios asignados | | Trasladan los inventarios de activos en formatos técnicos |
| | | | Se lleva a cabo los inventarios de activos de soporte de software |

Fuente: Autoría Propia

Tabla 13. Vulnerabilidades en el componente Seguridad de los Recursos Humanos.

| SEGURIDAD DE LOS RECURSOS HUMANOS | | | |
|--|--|---|---|
| Vulnerabilidades | | | |
| Cumple | Cumple a medias | Cumple sin Evidencias | No Cumple |
| Se relacionan los procedimientos de mantenimiento correctivo, preventivo de los bienes: Software, Hardware y equipos de comunicación | El personal que trabaja en el departamento de informática son los adecuados para cumplir las necesidades de este | El departamento de tecnología tiene restringido con claridad sus responsabilidades | Se posee objetivos para el departamento de tecnología |
| Se atribuye o notifica al personal del mal uso y destrucción de los equipos tecnológicos asignados | | Bajo qué criterios existe la falta de cumplimiento de sus funciones | Posee definido por escrito los objetivos del departamento de tecnología |
| | | Se efectúa la devolución de los equipos tecnológicos del personal que finaliza su contrato de trabajo por escrito | El departamento tecnológico posee conflictos por la carga de trabajo |

Fuente: Autoría Propia

Tabla 14. Vulnerabilidades en el componente Seguridad Física del Entorno.

| SEGURIDAD FISICA DEL ENTORNO | | | |
|------------------------------|-----------------|-----------------------|-----------|
| Vulnerabilidades | | | |
| Cumple | Cumple a medias | Cumple sin Evidencias | No cumple |

| | | | |
|---|--|--|--|
| <p>Posee un registro del equipo o activo se ha retirado o cuando se ha devuelto</p> | | <p>Se encuentran los repuestos y soportes de los equipos a una distancia prudente para evitar daños en caso de desastre de las</p> | <p>Se posee un control de mantenimientos periódicos de los dispositivos tecnológicos y los equipos de acuerdo a las especificaciones y</p> |
| | | <p>instalaciones principales</p> | <p>recomendaciones del proveedor</p> |
| | | <p>Se ubica el equipo apropiado contra incendios</p> | <p>Se guardan registros de los mantenimientos correctivos, preventivos, fallas relevantes o sospechosas</p> |
| | | <p>Se efectúan mantenimientos de las instalaciones eléctricas y ups</p> | <p>Se constituyen controles de mantenimientos programados</p> |
| | | <p>Se efectúan mantenimientos de los sistemas de climatización y ductos de ventilación</p> | <p>Se establece un registro de los mantenimientos correctivos y a su vez los preventivos</p> |
| | | <p>Se posee protección contra variaciones de energía o descargas eléctricas en las edificaciones de la institución</p> | <p>Posee custodia los equipos y medios que se encuentran fuera de la institución</p> |
| | | <p>Existen garantías físicas para trabajar en las áreas seguras</p> | <p>Posee cobertura de seguro para proteger los equipos que se encuentran fuera de la institución</p> |
| | | <p>Los equipos se encuentran correctamente ubicados o protegidos de las amenazas o peligros del entorno</p> | <p>Posee un manual de borrado para equipos con información sensible o reutilizado</p> |

| | | | |
|--|--|--|--|
| | | Se da seguimiento de las condiciones ambientales de humedad y temperatura | |
| | | Se posee protección contra variaciones de energía o descargas eléctricas en las edificaciones de la institución | |
| | | Se posee protección contra variaciones de energía o descargas eléctricas en las edificaciones de la institución | |
| | | Se posee filtros protectores en las líneas de comunicación y en el suministro de energía | |
| | | Se garantiza el cableado de energía de los cables de red | |
| | | Se separan los cables de energía de los cables de red | |
| | | Se separan los cables de energía de los cables de red según los estándares para el correcto funcionamiento de la red en el Data Center | |
| | | Se establecen las normativas locales e internacionales para la implementación de las redes | |

| | | | |
|--|--|---|--|
| | | Se dispone de documentación, planos, diseños, de la distribución de todas conexiones de redes alámbricas e inalámbricas | |
| | | El personal calificado y autorizado realiza los mantenimientos de los equipos tecnológicos | |
| | | Posee control de acceso para las redes inalámbricas del establecimiento | |
| | | Posee control de acceso a los servidores | |
| | | Posee un formulario de evaluación a los dispositivos deteriorados que contengan información sensible antes de enviar a reparación | |
| | | Posee la autorización necesaria previa para el retiro de cualquier equipo, información o software | |
| | | Poseen identificación las personas autorizadas para el retiro de los activos del establecimiento | |

Fuente: Autoría Propia

Tabla 15. Vulnerabilidades en el componente Gestión de Comunicación y Operación.

| |
|--|
| GESTION DE COMUNICACION Y DE OPERACION |
| Vulnerabilidades |

| Cumple | Cumple a medias | Cumple sin Evidencias | No cumple |
|---|-----------------|--|---|
| Posee políticas de respaldo de la información antes del mantenimiento | | Posee distribución de responsabilidades y funciones en el Departamento Tecnológico | Posee documentación del proceso de respaldo y restauración de la información |
| | | Posee gestiones de escalabilidad para asegurar el desempeño requerido de los servicios y sistemas informáticos | Posee documentación de los procedimientos para el reinicio y recuperación del sistema en caso de fallas |
| | | Posee un bloqueo de software no autorizado o ajenos a terceros para la institución | Posee documentación de los procedimientos para el reinicio y recuperación del sistema en caso de fallas |
| | | Posee instalación y actualización automática de software de antivirus contra código malicioso | Posee programación del proceso de cambio con su prueba correspondiente |
| | | Se posee los sistemas operativos actualizados con las últimas versiones estable | Se delegan responsables de control de cambios en los equipos tecnológicos y software |
| | | Denominan responsabilidades y procedimientos para la asistencia de equipos remotos | Se aprueban de manera formal los cambios propuestos |
| | | Hacen diseños, planos antes de la implementación de una red | Las áreas de redes y mantenimiento se encuentran separadas |
| | | Se verifican fallas o alertas del sistema operativo | |

| | | | |
|--|--|---|--|
| | | Se efectúan cambios de configuración de seguridad del sistema operativo | |
|--|--|---|--|

Fuente: Autoría Propia

Tabla 16. Vulnerabilidades en el componente Control de Acceso.

| CONTROL DE ACCESO | | | |
|--|-----------------|--|--|
| Vulnerabilidades | | | |
| Cumple | Cumple a medias | Cumple sin Evidencias | No cumple |
| Se documenta y encuentran identificados los equipos de las redes | | Posee documentada la identificación de todos los equipos que permitidos de la red | Se implementan procedimientos para controlar la instalación de software en sistemas operativos |
| | | Se implementan procedimientos para controlar la instalación de software en sistemas operativos | Posee un registro de las actualizaciones de software que se realizan, tipo auditoria |
| | | Posee documentación del control de versiones para todas las actualizaciones de software | |

Tabla 17. Vulnerabilidades en el componente Cumplimiento

| CUMPLIMIENTO | | | |
|------------------|-----------------|-----------------------|-----------|
| Vulnerabilidades | | | |
| Cumple | Cumple a medias | Cumple sin Evidencias | No cumple |
| | | | |

| | | | |
|--|--|--|--|
| | | | Se posee inventario de todas las normas legales, estatutos y reglamentos pertinentes para cada programa de software, servicio informático e información que utilice el establecimiento |
| | | | Posee conocimiento de las leyes y normas generales |
| | | | relacionadas a la gestión de datos e información electrónica relacionadas a la gestión de los datos. |

Fuente: Autoría Propia

La cantidad de riesgos encontrados para cada componente se resume en la Tabla 20 mostrada a continuación. Se puede visualizar que el componente de *Recursos Humanos* es el que posee mayor riesgo con un 46%, mientras que el componente *Control de Acceso* posee un riesgo del 23%.

Tabla 18. Porcentaje de Riesgo de componentes de la norma ISO 27001.

| Componentes | Nivel de riesgo | riesgos identificados | Porcentaje riesgo |
|----------------------------|-----------------|-----------------------|-------------------|
| Inventario de activo | Crítico | 2 | 11,9% |
| | Alto | 2 | |
| | Medio | 3 | |
| | Bajo | 0 | |
| | Total | 7 | |
| Seguridad recursos humanos | Crítico | 0 | 11,9% |
| | Alto | 4 | |
| | Medio | 2 | |
| | Bajo | 1 | |
| | Total | 7 | |
| | Crítico | 6 | |
| | Alto | 9 | |

| | | | |
|----------------------------------|---------|----|---------|
| Seguridad física de los entornos | Medio | 9 | 44,44% |
| | Bajo | 4 | |
| | Total | 28 | |
| Gestión comunicación y operación | Crítico | 2 | 25,39% |
| | Alto | 10 | |
| | Medio | 3 | |
| | Bajo | 0 | |
| | Total | 16 | |
| Control de Acceso | Crítico | 2 | 6,35% |
| | Alto | 1 | |
| | Medio | 1 | |
| | Bajo | 0 | |
| | Total | 4 | |
| Cumplimiento | Crítico | 1 | 2,05% |
| | Alto | 1 | |
| | Medio | 0 | |
| | Bajo | 0 | |
| | Total | 2 | |
| Total de riesgos | | 63 | 100,00% |

Fuente: Autoría Propia

Finalmente, los resultados del diagnóstico realizado sirvieron como base para diseñar las Matrices de Riesgos de cada uno de los componentes según norma ISO/IEC 27001. Dichas matrices se presentan a continuación en las Tablas 21, 22, 23, 24, 25 y 26 (Inventario de activo, Seguridad de los recursos humanos, Seguridad física de los entornos; Gestión de la comunicación y operación, Control de Acceso, y Cumplimiento; respectivamente).

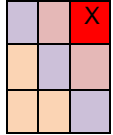
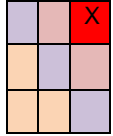
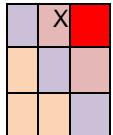
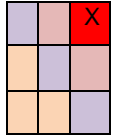
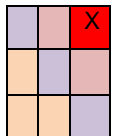
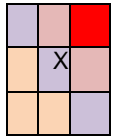
Tabla 1. Matriz de Riesgos basado en el componente Inventario de Activo según norma ISO/IEC 27001.

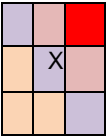
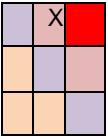
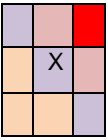
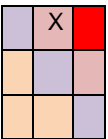
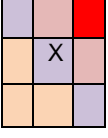
| ID. Riesgo | Vulnerabilidades | Probabilidad | Impacto | Nivel | Matriz de Riesgos | Responsables | ID de Mitigación | Acciones de mitigación | Criterio de aceptación |
|------------|---|--------------|----------------|---------|-------------------|---------------------------|------------------|---|----------------------------|
| R.1.1. | Se cuenta con un Plan Estratégico | Alto 3 | Muy Grave 3 | Crítico | | Directora/Coordinadora TI | A.1.1.1 | Elaborar un plan estratégico que contenga estrategias alineadas a los objetivos | Continuidad del negocio |
| R.1.2. | Se lleva un control de los inventario de los activos en formatos físicos | Alto 3 | Grave 2 | | | | | | |
| R.1.3. | No se llevan los inventarios de los activos de soporte de software | Alto 3 | Muy Grave 3 | Crítico | | Directora/Coordinadora TI | A.1.3.1 | Realizar registros de inventario de activos que han tenido soporte cada 3 meses | Actualización de registros |
| R.1.4. | Se lleva un control los inventarios de los activos de soporte de software | Alto 3 | Menor 1 | | | | | | |
| R.1.5. | Se lleva control los inventarios de los activos de soporte de redes | Medio 2 | Grave 2 | Medio | | Directora/Coordinadora TI | A.1.5.1 | Cumplir la totalidad del registro de soporte de activos de redes | Actualización de registros |
| R.1.6. | Existen activos o grupos de activos que no poseen custodios asignados | Alto 3 | Grave 2 | | | | | | |

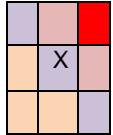
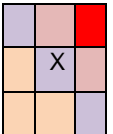
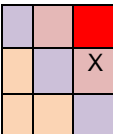
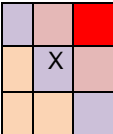
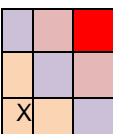
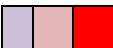
Tabla 2. Matriz de Riesgos basado en el componente Seguridad de los Recursos Humanos según norma ISO/IEC 27001.

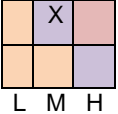
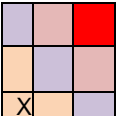
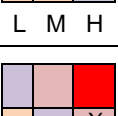
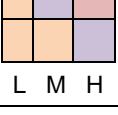
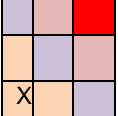
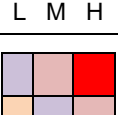
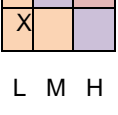
| ID. Riesgo | Vulnerabilidades | Probabilidad | Impacto | Nivel | Matriz de Riesgos | Responsables | ID de Mitigación | Acciones de mitigación | Criterio de aceptación |
|------------|--|--------------|----------------|-------|-------------------|--------------------------|------------------|---|--|
| R.2.1. | Se posee objetivos para el departamento de tecnología | Alto 3 | Grave 2 | Alto | | Directora/Coordinador TI | A.2.1.1 | Entablar objetivos del departamento para una mejor productividad | Políticas, Planes y procedimientos del departamento. |
| R.2.2. | Posee definido por escrito los objetivos del departamento de tecnología | Medio 2 | Grave 2 | Medio | | Directora/Coordinador TI | A.2.1.2 | Aprobación de los objetivos del departamento TI, socializando con el resto del personal | Integridad de la información departamento TI |
| R.2.3. | El departamento tecnológico posee conflictos por la carga de trabajo | Alto 3 | Grave 2 | Alto | | Directora/Coordinador TI | A.2.1.3 | La directora de TI debe segregar funciones al personal. | Ambiente laboral estable |
| R.2.4. | El departamento de tecnología tiene restringido con claridad sus responsabilidades | Alto 2 | Menor 3 | Alto | | Directora/Coordinador TI | A.2.1.4 | Elaborar un manual de funciones y responsabilidades para el departamento TI | Mejorar el ambiente laboral |
| R.2.5. | Se atribuye o notifica al personal del mal uso y destrucción de los equipos tecnológicos asignados | Medio 3 | Grave 2 | Alto | | Directora/Coordinador TI | A.2.1.5 | Contratar personal capacitado en TI | Mejorar el ambiente laboral |
| R.2.6. | El personal que trabaja en el departamento de informática son los adecuados para cumplir las necesidades de este | Medio 2 | Muy Grave 3 | Alto | | Directora/Coordinador TI | A.2.1.6 | Capacitar o seleccionar al mejor personal para las necesidades requeridas | Capacidad laboral |

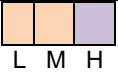
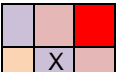
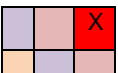
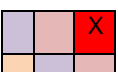
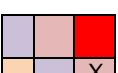
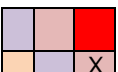
Tabla 3. Matriz de Riesgos basado en el componente Seguridad Física del Entorno según norma ISO/IEC 27001

| ID. Riesgo | Vulnerabilidades | Probabilidad | Impacto | Nivel | Matriz de Riesgos | Responsables | ID de Mitigación | Acciones de mitigación | Criterio de aceptación |
|------------|---|--------------|----------------|---------|---|-------------------------------|------------------|--|------------------------|
| R.3.1. | Se posee un control de mantenimientos periódicos de los dispositivos tecnológicos y los equipos de acuerdo a las especificaciones y recomendaciones del proveedor | Alto 3 | Muy Grave 3 | Crítico |  L M H | Directora TI | A.3.1.1 | Mantenimientos periódicos de equipos y dispositivos según las especificaciones y recomendaciones del proveedor | Mejora de los procesos |
| R.3.2. | Se guardan registros de los mantenimientos correctivos, preventivos, fallas relevantes o sospechosas | Alto 3 | Muy Grave 3 | Crítico |  L M H | Directora TI | A.3.2.1 | Mantener áreas seguras los registros de los mantenimientos | Mejora de los procesos |
| R.3.3. | Se constituyen controles de mantenimientos programados | Medio 2 | Muy Grave 3 | Alto |  L M H | Directora TI- Áreas asignadas | A.3.3.1 | Crear controles de mantenimientos cada 6 meses | Control |
| R.3.4. | Posee un registro de los mantenimientos correctivos y preventivos | Alto 2 | Muy Grave 3 | Crítico |  L M H | Directora TI | A.3.4.1 | Programar registros de mantenimientos | Seguridad |
| R.3.5. | Posee custodio los equipos y medios que se encuentran fuera de la institución | Alto 3 | Grave 2 | Alto |  L M H | Directora TI | A.3.5.1 | Disponer de custodios para los equipos que están dentro y fuera de la institución | Control |
| R.3.6. | Posee cobertura de seguro para proteger los equipos que se encuentran fuera de la institución | Medio | Grave | Medio |  L M H | Directora TI | A.3.6.1 | Determinar cobertura de seguro para la protección de los equipos que están fuera de la institución | Control |

| | | | | | | | | | |
|--------|---|-------|-----------|-------|---|------------------------------|----------|--|-----------|
| | | 2 | 3 | | | | | | |
| R.3.7. | Posee un formulario de evaluación a los dispositivos deteriorados que contengan información sensible antes de enviar a reparación | Medio | Grave | Medio |  L M H | Directora TI | A.3.7.1 | Usar técnicas de borrado seguro | Ejecución |
| | | 2 | 2 | | | | | | |
| R.3.8 | Se encuentran los repuestos y soportes de los equipos a una distancia prudente para evitar daños en caso de desastre de las instalaciones principales | Medio | Muy Grave | Alto |  L M H | Directora TI-Áreas asignadas | A.3.8.1 | Mantener repuestos en lugares que no puedan sufrir daños en caso de desastres | Seguridad |
| | | 2 | 3 | | | | | | |
| R.3.9. | Se ubica el equipo apropiado contra incendios | Medio | Grave | Medio |  L M H | Directora TI | A.3.9.1 | Establecer los equipos contra incendios sean apropiados para TI | Control |
| | | 2 | 2 | | | | | | |
| R.3.10 | Se efectúan mantenimientos de las instalaciones eléctricas y ups | Medio | Muy Grave | Alto |  L M H | Directora TI-Áreas asignadas | A.3.10.1 | Registrar los mantenimientos para llevar detalles de los fallos de los equipos | Seguridad |
| | | 2 | 3 | | | | | | |
| R.3.11 | Los equipos tecnológicos cuentan con protección contra fallas de suministro de energía | Medio | Grave | Medio |  L M H | Directora TI | A.3.11.1 | Implementar sistema de alertas para los sistemas de información | Control |
| | | 2 | 2 | | | | | | |

| | | | | | | | | | |
|--------|---|-------|-----------|-------|--|------------------------------|----------|---|-----------|
| R.3.12 | Se efectúan mantenimientos de los sistemas de climatización y ductos de ventilación | Medio | Grave | Medio |  | Directora TI | A.3.12.1 | Llevar los registros de mantenimientos en los sistemas y climatización y ductos de ventilación | Control |
| | | 2 | 2 | | L M H | | | | |
| R.3.13 | Se establecen controles para minimizar el riesgo de amenazas físicas, tales como robo, incendio, entre otras | Medio | Grave | Medio |  | Directora TI | A.3.13.1 | Realizar registros de control de riesgos para minimizar amenazas físicas, robo, incendio, interferencia | Control |
| | | 2 | 2 | | L M H | | | | |
| R.3.14 | Existen garantías físicas para trabajar en las áreas seguras | Medio | Muy Grave | Alto |  | Directora TI-Áreas asignadas | A.3.14.1 | Elaborar un diseño de seguridad y protección físicas de las áreas seguras | Ejecución |
| | | 2 | 2 | | L M H | | | | |
| R.3.15 | Se encuentran los repuestos y soportes de los equipos a una distancia prudente para evitar daños en caso de desastre de las instalaciones principales | Medio | Grave | Medio |  | Directora TI | A.3.15.1 | Ubicar los equipos en lugares seguros para reducir el riesgo de peligros del entorno | Seguridad |
| | | 2 | 2 | | L M H | | | | |
| R.3.16 | Se monitorean las condiciones ambientales de temperatura y humedad, pero no hay reportes de control | Bajo | Menor | Bajo |  | Directora TI | A.3.16.1 | Controlar la temperatura ambiental y la humedad para que los equipos no sufran daños o deterioros en su funcionalidad | Seguridad |
| | | 1 | 1 | | L M H | | | | |
| | Los equipos tecnológicos cuentan | Medio | Grave | |  | Directora TI | | Registrar edificaciones seguras contra | |

| | | | | | | | | | |
|--------|--|-------|-----------|---------|---|--------------|----------|---|---------------------|
| R.3.17 | con protección contra fallas de suministro de energía | | | Medio |  | | A.3.17.1 | descargas eléctricas | Seguridad |
| | | 2 | 2 | | L M H | | | | |
| R.3.18 | Se posee filtros protectores en las líneas de comunicación y en el suministro de energía | Bajo | Menor | Bajo |  | Directora TI | A.3.18.1 | Usar filtros protectores del suministro de energía | Seguridad |
| | | 1 | 1 | | L M H | | | | |
| R.3.19 | Se posee protección contra variaciones de energía o descargas eléctricas en las edificaciones de la institución | Alto | Grave | Alto |  | Directora TI | A.3.19.1 | Acoger equipos tecnológicos contra fallas de energía | Seguridad |
| | | 3 | 2 | | L M H | | | | |
| R.3.20 | Se garantiza el cableado de energía de los cables de red | Bajo | Menor | Bajo |  | Directora TI | A.3.20.1 | Acoger cableado de la red | Seguridad |
| | | 1 | 1 | | L M H | | | | |
| R.3.21 | Se separan los cables de energía de los cables de red según los estándares para el correcto funcionamiento de la red en el Data Center | Bajo | Menor | Bajo |  | Directora TI | A.3.21.1 | Usar diferentes canales para los cables de energía de los cables de red | Seguridad |
| | | 1 | 1 | | L M H | | | | |
| R.3.22 | Se llevan las normas locales e internacionales para la implementación de las redes, parcialmente | Alto | Muy Grave | Crítico |  | Directora TI | A.3.22.1 | Acoger normativa CGE 410-09 TI | Mejora la seguridad |
| | | 1 | 1 | | L M H | | | | |
| R.3.23 | Se dispone de documentación, planos, diseños, de la distribución de todas | Medio | Grave | |  | Directora TI | A.3.23.1 | Disponer la información, documentos, diseños, planos, distribución de | Control |
| | | | | | | | | | |

| | | | | | | | | | |
|--------|---|-------|-----------|---------|--|-----------------|----------|--|-----------|
| | conexiones de redes alámbricas e inalámbricas de redes inalámbricas y alámbricas, no están disponibles | 2 | 2 | Medio |  | | | red | |
| R.3.24 | Posee la autorización necesaria previa para el retiro de cualquier equipo, información o software | Bajo | Menor | Bajo |  | Directora TI | A.3.24.1 | Disponer de personal debidamente capacitado para los mantenimientos de los equipos | Control |
| | | 1 | 1 | | | | | | |
| R.3.25 | Posee control de acceso para las redes inalámbricas del establecimiento | Alto | Muy Grave | Crítico |  | Directora TI | A.3.25.1 | Gestionar control de acceso de las redes inalámbricas | E |
| | | 3 | 3 | | | | | | |
| R.3.26 | Posee control de acceso a los servidores | Alto | Muy Grave | Crítico |  | Directora TI | A.3.26.1 | Gestionar controles de acceso a los servidores | Seguridad |
| | | 3 | 3 | | | | | | |
| R.3.27 | Posee un formulario de evaluación a los dispositivos deteriorados que contengan información sensible antes de enviar a reparación | Medio | Muy Grave | Alto |  | Directora de TI | A.3.27.1 | Efectuar evaluación de equipos deteriorados o con fallas que posean información sensible | Control |
| | | 2 | 3 | | | | | | |
| R.3.28 | Posee la autorización necesaria previa para el retiro de cualquier equipo, información o software | Alto | Grave | Alto |  | Directora TI | A.3.28.1 | Gestionar autorización o personal esencial para el retiro de equipos. | Control |
| | | 3 | 2 | | | | | | |

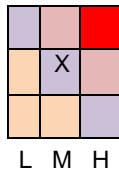
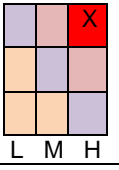
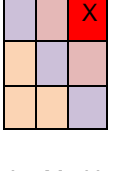
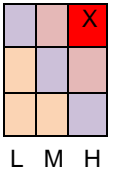
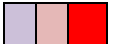
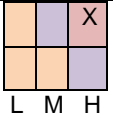
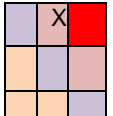
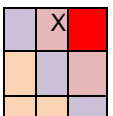
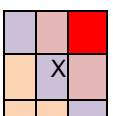
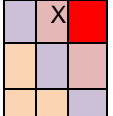
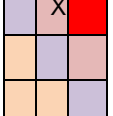
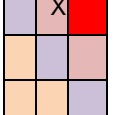
| | | | | | | | | | |
|--------|--|-------|-------|------|--|--------------|----------|---|-----------|
| R.3.29 | Poseen identificación las personas autorizadas para el retiro de los activos del establecimiento | Medio | Grave | Alto |  | Directora TI | A.3.29.1 | Retirar activos de la institución debe ser través de actas de entrega recepción, e identificando al personal quien lo va a retirar. | Seguridad |
| | | 2 | 2 | | | | | | |

Tabla 4. Matriz de Riesgos basado en el componente Gestión de Comunicación y Operación según norma ISO/IEC 27001

| ID. Riesgo | Vulnerabilidades | Probabilidad | Impacto | Nivel | Matriz de Riesgos | Responsables | ID de Mitigación | Acciones de mitigación | Criterio de aceptación |
|------------|--|--------------|-----------|---------|--|--------------|------------------|---|------------------------|
| R.4.1. | Posee documentación del proceso de respaldo y restauración de la información | Alto | Muy Grave | Crítico |  | Directora TI | A.4.1 | Tomar medidas de documentación del proceso de respaldo y restauración de la información | Control |
| | | 3 | 3 | | | | | | |
| R.4.2. | Posee documentación o instrucciones para el manejo de errores y otras condiciones que pueden surgir mediante ejecución de tareas | Alto | Muy Grave | Crítico |  | Directora TI | A.4.2 | Tomar medidas de Documentación de los errores y otras fallas que se presentan en la ejecución de tareas | Control |
| | | 3 | 3 | | | | | | |
| R.4.4. | Posee documentación de los procedimientos para el reinicio y recuperación del sistema en caso de fallas | Alto | Muy Grave | Crítico |  | Directora TI | A.4.4 | Tomar medidas de documentación de los procedimientos para el inicio y recuperación del sistema | Control |
| | | 3 | 3 | | | | | | |
| | Posee programación del proceso de | Alto | Muy Grave | |  | | | Realizar planificaciones de los cambios que se | |

| | | | | | | | | | |
|--------|--|-------|-----------|-------|--|--------------|--------|--|---------------------|
| R.4.5. | cambio con su prueba correspondiente | 2 | 3 | Alto |  | Directora TI | A.4.5 | realizan en cada prueba | Ejecución |
| R.4.6. | Se delegan responsables de control de cambios en los equipos tecnológicos y software | Alto | Grave | Alto |  | Directora TI | A.4.6 | Delegar la formalidad en los cambios de equipos y software estableciendo una persona a cargo | Ejecución |
| | | 3 | 2 | | | | | | |
| R.4.7. | Se autorizan de manera formal los cambios o recomendaciones propuestas | Medio | Muy Grave | Alto |  | Directora TI | A.4.7 | Gestionar los cambios para que haya formalidad en el proceso | Ejecución |
| | | 2 | 3 | | | | | | |
| R.4.8. | Las áreas de redes y mantenimiento se encuentran separadas | Medio | Grave | Medio |  | Directora TI | A.4.8 | Cada áreas del departamento deben mantenerse separadas | Seguridad |
| | | 2 | 2 | | | | | | |
| R.4.9. | Posee distribución de responsabilidades y funciones en el Departamento Tecnológico | Medio | Muy Grave | Alto |  | Directora TI | A.4.9 | Delegar funciones de acuerdo al perfil del empleado | Control |
| | | 2 | 3 | | | | | | |
| R.4.10 | Posee gestiones de escalabilidad para asegurar el desempeño requerido de los servicios y sistemas informáticos | Medio | Muy Grave | Alto |  | Directora TI | A.4.10 | Generar indicadores de desempeño de los sistemas y servicios informáticos | Control |
| | | 2 | 3 | | | | | | |
| R.4.11 | Posee un bloqueo de software no autorizado o ajenos a terceros para la institución | Medio | Muy Grave | Alto |  | Directora TI | A.4.11 | Gestionar el control del uso de software no autorizado | Control y Seguridad |
| | | 2 | 3 | | | | | | |

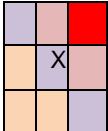
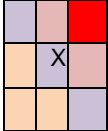
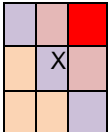
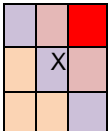
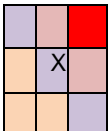
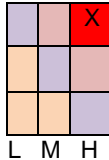
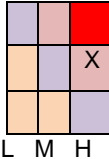
| | | | | | | | | | |
|--------|---|-------|-----------|-------|--|-----------------|--------|--|------------------------|
| R.4.12 | Posee instalación y actualización automática de software de antivirus contra código malicioso | Medio | Grave | Medio |  L M H | Directora TI | A.4.12 | Realizar programas de actualización periódica de antivirus contra código malicioso | Seguridad |
| | | 2 | 2 | | | | | | |
| R.4.13 | Denominan responsabilidades y procedimientos para la asistencia de equipos remotos | Medio | Muy Grave | Alto |  L M H | Directora TI | A.4.13 | Designar responsabilidades para la asistencia de equipos remotos de acuerdo al manual de procedimiento | Control |
| | | 2 | 3 | | | | | | |
| R.4.14 | Hacen diseños, planos antes de la implementación de una red | Medio | Muy Grave | Medio |  L M H | Directora TI | A.4.14 | Elaborar y documentar diseños de red antes de su implementación | Seguridad de Redes |
| | | 2 | 3 | | | | | | |
| R.4.15 | Se verifican fallas o alertas del sistema operativo | Medio | Muy Grave | Alto |  L M H | Directora TI | A.4.15 | Gestionar sistema de alertas para mantener actualizaciones del sistema operativo | Ejecución |
| | | 2 | 3 | | | | | | |
| R.4.16 | Se efectúan cambios de configuración de seguridad del sistema operativo | Medio | Muy Grave | Alto |  L M H | Directora TI | A.4.16 | Configurar los accesos de seguridad del sistema operativo | Seguridad y Control |
| | | 2 | 3 | | | | | | |

Tabla 5. Matriz de Riesgos basado en el componente Control de Acceso según norma ISO/IEC 27001

| ID. Riesgo | Vulnerabilidades | Probabilidad | Impacto | Nivel | Matriz de Riesgos | Responsables | ID de Mitigación | Acciones de mitigación | Criterio de aceptación |
|------------|--|--------------|----------------|-------|-------------------|--------------|------------------|--|------------------------|
| R.5.1. | Se implementan procedimientos para controlar la instalación de software en sistemas operativos | Alto 3 | Grave 2 | Alto | | Directora TI | A.5.1 | Gestionar procedimientos para el uso de software. | Antivirus |
| R.5.2. | Posee un registro de las actualizaciones de software que se realizan, tipo auditoria | Alto 3 | Grave 2 | Alto | | Directora TI | A.5.2 | Gestionar lista de control de auditoria que se hacen en la actualización del software. | Control |
| R.5.3. | Se documenta y encuentran identificados los equipos de las redes | Medio 2 | Muy Grave 3 | Alto | | Directora TI | A.5.3 | Gestionar documentación de los equipos permitidos, según la red a la que pertenecen | Registros documental |
| R.5.4. | El sistema operativo posee restricciones de cambios o instalación de paquetes de software | Alto 3 | Menor 1 | Medio | | Directora TI | A.5.4 | Restringir acceso a configuraciones para denegar los cambios de paquetes de software | Seguridad |
| R.5.5. | Posee documentación del control de versiones para todas las actualizaciones de software | Medio 2 | Grave 2 | Medio | | Directora TI | A.5.5 | Llevar control de versiones actualizadas de software | Control |

Tabla 6. Matriz de Riesgos basado en el componente Cumplimiento según norma ISO/IEC 27001

| ID. Riesgo | Vulnerabilidades | Probabilidad | Impacto | Nivel | Matriz de Riesgos | Responsables | ID de Mitigación | Acciones de mitigación | Criterio de aceptación |
|------------|--|--------------|---------|---------|---|--------------|------------------|---|---|
| R.6.1. | Se posee inventario de todas las normas legales, estatutos y reglamentos pertinentes para cada programa de software, servicio informático e información que utilice el establecimiento | Alto | Grave | Crítico |  L M H | Directora TI | A.6.1 | Acoger la normativa de Contraloría General del Estado 410-09, además de las normativas internacionales ISO 27001 para asegurar la información | Normativa para la seguridad de la información |
| | | 3 | 3 | | | | | | |
| R.6.2. | Posee conocimiento de las leyes y normas generales relacionadas a la gestión de datos e información electrónica | Alto | Grave | Alto |  L M H | Directora TI | A.6.2 | Capacitar al personal esencial de TI sobre las leyes que se están rigiendo para la gestión de información | Regulación de la normativa |
| | | 3 | 2 | | | | | | |

Explicación de Matriz de Riesgo

Cada componente posee su Matriz de riesgo con sus respectivos ítems detallados a continuación:

ID. Riesgo: Corresponde a cada ítem según su orden en las tablas anteriores, tomando en cuenta el componente, por ejemplo.

Tabla 25 ID de Riesgo

| Componente | ID |
|-------------------------------------|----|
| Inventario de Activo | R1 |
| Seguridad de los Recursos Humanos | R2 |
| Seguridad Física | R3 |
| Gestión de Comunicación y Operación | R4 |
| Control de Acceso | R5 |
| Control de Acceso | R6 |

Fuente: Autoría Propia

Vulnerabilidades: Hace referencia al componente evaluado.

Probabilidad: Corresponde a la concurrencia a la que suele suceder la vulnerabilidad.

Impacto: De nota lo importante que es esa vulnerabilidad, su nivel de impacto o importancia.

Nivel y matriz de riesgos: De acuerdo a la tabla 20 porcentaje de riesgo de componentes de la norma los niveles se encuentran divididos en los siguientes sectores y colores:

| Nivel de riesgo |
|-----------------|
| Crítico |
| Alto |
| Medio |
| Bajo |

Figure 16 Nivel de riesgo

Responsables: Hace referencia al área asignada donde se encuentra dicha vulnerabilidad.

Acciones de mitigación: Recomendación o acción para solventar la vulnerabilidad de acuerdo a las normas.

Criterio de aceptación: Definen los requisitos o bases para la aceptación de la vulnerabilidad.

Explicación tabla 20 Matriz de Riesgos basado en el componente Inventario de Activo.

De acuerdo a la antes mencionada matriz esta cuenta con 10 ítems, las cuales cuentan con ID de Riesgo para identificarlas, vulnerabilidades las cuales el 80% de estas constan con una probabilidad de concurrencia **ALTA** con las que suele suceder dichas vulnerabilidades, posee 3 vulnerabilidades con impacto **GRAVE**, 2 **MUY GRAVE** y 1 **MENOR**, con niveles de riesgo de tipo **CRITICO**, **ALTO** y **MEDIO** según el semáforo explicado en la tabla 20, Responsables el cual en este caso recae sobre la Directora de TIC, ID de mitigación que se representa de forma secuencial al ID de Riesgo por ejemplo **A.1.1.1**, **A.1.2.1**, etc. también cuenta con un Ítem de Acciones de Mitigación donde posee una recomendación o acción de acuerdo a todos los datos recolectados basado en la norma iso 27001 y por ultimo Criterio de aceptación donde se define la aceptación de la vulnerabilidad de acuerdo a las bases o requisito como por ejemplo. De la vulnerabilidad **Se lleva un control del inventario de los activos en formatos físicos** posee como criterio de aceptación **Constancia de los activos del departamento TI**.

Explicación tabla 21 Matriz de Riesgos basado en el componente Seguridad de los Recursos Humanos según norma

La Matriz de riesgo basado en el componente de seguridad de los recursos humanos consta de 6 vulnerabilidades con sus respectivo id de riesgo el cual entre los principales son: **El departamento tecnológico posee conflictos por la carga de trabajo**, **El departamento de tecnología tiene restringido con claridad sus responsabilidades**. Cada uno con respectivo ID, en el cual de las 6 vulnerabilidades posee 3 con probabilidad **ALTA** y 3 con probabilidad **MEDIO**, con un índice de impacto de 4 **GRAVE**, 1 **MUY GRAVE** y 1 **MENOR**. Su nivel de riesgo es de 5 **ALTOS** y 1 **MEDIO**, responsabilidad exclusiva de la Directora de TIC con su respectivo ID de mitigación, entre las principales acciones de mitigación se encuentra las de **la directora de TI debe segregar funciones al personal**, **Elaborar un manual de funciones y responsabilidades para el departamento TI** poseyendo los siguientes criterios de aceptación **Ambiente laboral estable** y **Mejorar el ambiente laboral**.

Explicación de la tabla 22 Matriz de Riesgos basado en el componente Seguridad Física del Entorno.

De acuerdo a la tabla 23 de la matriz de riesgos basado en el componente seguridad física del entorno este cuenta con 29 vulnerabilidades con su respectivos ID como por ejemplo **R.3.3**, **R.3.4**, **R.3.5**, entre las principales vulnerabilidades y más importantes están las siguientes: **Se constituyen controles de mantenimientos programados**, **Posee un registro de los mantenimientos correctivos y preventivos**, **Posee custodio los equipos y medios que se encuentran fuera de la institución**. De los cuales estos poseen una probabilidad de **MEDIO**, **ALTO** y **ALTO** con un impacto de **MUY GRAVE**, **MUY GRAVE** y **GRAVE** y sus niveles de riesgo **ALTO**, **CRITICO** y **ALTO** el cual se encuentran representado según el semáforo en la figura 16. Su responsable a cargo la directora de tic, poseen las siguientes acciones de mitigación: **Crear controles de mantenimientos cada 6 meses**, **Programar registros de mantenimientos**, **Disponer de custodios para los equipos que están dentro y fuera de la institución**. Para cada una de las vulnerabilidades descritas anteriormente comprenden un criterio de aceptación como lo son: **Control**, **Seguridad** y **Control**.

Explicación de la tabla 23 Matriz de riesgos basado en la gestión de comunicación y operación.

Según la tabla 24 de la matriz de riesgos basado en la gestión de comunicación y operación cuenta con un total de 16 vulnerabilidades con su respectivo ID de riesgo de los cuales poseen una totalidad de probabilidad de 11 **MEDIO** y 5 **ALTO**, manejando un impacto total de 12 **MUY GRAVE** y 4 **GRAVE**, mientras que sus totales de niveles de riesgo son de 9 **ALTO**, 4 **CRITICO** y 3 **MEDIO**. Su responsable a cargo la directora de tic, entre las vulnerabilidades más importantes se encuentran las siguientes: Posee documentación del proceso de respaldo y restauración de la información, Se delegan responsables de control de cambios en los equipos tecnológicos y software, Se autorizan de manera formal los cambios o recomendaciones propuestas. De las cuales sus acciones a mitigar son: **Tomar medidas de documentación del proceso de respaldo y restauración de la información, Delegar la formalidad en los cambios de equipos y software estableciendo una persona a cargo, Gestionar los cambios para que haya formalidad en el proceso.** Mientras que su criterio de aceptación son los siguientes: **Control, Ejecución, Ejecución.**

Explicación de la tabla 24 Matriz de Riesgos basado en el componente Control de Acceso.

De acuerdo a la tabla 25 Matriz de Riesgos basado en el componente Control de Acceso existen un total de 5 vulnerabilidades entre las cuales las principales a tomar en cuenta son: **Posee un registro de las actualizaciones de software que se realizan tipo auditoria, El sistema operativo posee restricciones de cambios o instalación de paquetes de software, Posee documentación del control de versiones para todas las actualizaciones de software** con su respectivo ID de Riesgo **R.5.2, R.5.4, R.5.5.** Las cuales cada una de estas poseen una probabilidad de concurrencia de **ALTO, ALTO, MEDIO** y un impacto **GRAVE, MENOR Y GRAVE**. Mientras que su nivel de riesgo es **ALTO, MEDIO, MEDIO** diagramado según el semáforo en la figura 16. El área o dirección encargado es la **dirección de TIC**, al igual que cada uno de estos posee acciones a mitigar, tales como: **Gestionar lista de control de auditoria que se hacen en la actualización del software, Restringir acceso a configuraciones para denegar los cambios de paquetes de software, Llevar control de versiones actualizadas de software.** Y sus criterios de aceptación **control, seguridad, control.**

Explicación de la tabla 25 Matriz de Riesgos basado en el componente Cumplimiento.

Según los datos recaudados para la generación de la matriz de riesgos en el componente cumplimiento tiene un total de 2 vulnerabilidades las cuales son: **Se posee inventario de todas las normas legales, estatutos y reglamentos pertinentes para cada programa de software, servicio informático e información que utilice el establecimiento, Posee conocimiento de las leyes y normas generales relacionadas a la gestión de datos e información electrónica** poseyendo los siguientes ID de riesgo **R.6.1, R.6.2,** con una

probabilidad de concurrencia de la vulnerabilidad de **ALTO, ALTO** y de un impacto **GRAVE, GRAVE**, con un nivel de riesgo **CRITICO, ALTO** diagramado en las tablas y figuras anteriores. Como área responsable se encuentra la **directora de TIC**, su ID de mitigación es **A.6.1, A.6.2**, con las siguientes acciones de mitigación: **Acoger la normativa de Contraloría General del Estado 410-09, además de las normativas internacionales ISO 27001 para asegurar la información, Capacitar al personal esencial de TI sobre las leyes que se están rigiendo para la gestión de información** y sus criterios de aceptación son: **Normativa para la seguridad de la información, Regulación de la normativa.**

CAPÍTULO 4

4. CONCLUSIONES Y TRABAJO FUTURO

La importancia de la implementación de un Sistema de gestión de la seguridad de la información basado en las normas ISO 27001 son varios entre ellos, el manejo de la seguridad informática a nivel institucional, la importancia de la identificación de las áreas a mejorar, la toma de acciones correctivas y efectivas.

Contar con un sistema de seguridad informática con la capacidad de proteger la infraestructura tecnológica, esencialmente la información contenida en un ordenador o circulante a través de las plataformas virtuales, es primordial para minimizar los riesgos de ataques a la infraestructura tecnológica. Por ello, la importancia de analizar todo respecto a la seguridad informática, establecer preguntas de investigación que permitan determinar si los sistemas cuentan con la gestión para minimizar los riesgos de futuros ataques informáticos, analizar las amenazas a las que se enfrentan los sistemas y equipos tecnológicos, es decir:

- ¿Cómo puede la Universidad Estatal de Milagro contar con la seguridad informática que le permita afrontar de manera satisfactoria los diferentes riesgos, así como prevenirlos, para mantener segura la infraestructura tecnológica?
- ¿Qué amenazas humanas pueden vulnerar la infraestructura tecnológica de la institución?
- ¿Determinar los riesgos de las amenazas lógicas que se pueden evidenciar y las diferentes amenazas físicas que se puedan presentar para violar la seguridad de la información?
- ¿Cómo establecer políticas de acceso para evitar que usuarios no autorizados puedan acceder a información confidencial dentro de la infraestructura tecnológica?
- ¿Cuáles son los recursos de mayor prioridad dentro de la organización que pueden ser afectados por un problema de seguridad?
- ¿De qué forma se podría generar conciencia en la comunidad universitaria acerca de temas de seguridad informática?

Establecer un análisis más amplio y claro de los posibles escenarios a los que se enfrentan las actividades administrativas y académicas, y qué puede hacerse para evitar riesgos y ataques a la infraestructura tecnológica.

Lo cual la principal necesidad surgió de desarrollar esta investigación con el propósito de evaluar la seguridad informática, bajo la Norma ISO 27001, en la infraestructura tecnológica de la Universidad Estatal de Milagro, lo que permitirá conocer el nivel de impacto que pueden tener la ocurrencia de las amenazas en cada activo de la infraestructura tecnológica, minimizar los riesgos existentes y, por ende, ayudar a fortalecer la confidencialidad, integridad y disponibilidad de la información.

Por lo tanto, un sistema de Gestión de Seguridad de la información genera un sentido de adecuación, adaptación y compromiso con respecto a la seguridad, la integración, participación y contribución de los distintos miembros de la institución en las diferentes etapas de su desarrollo.

4.1 CONCLUSIONES

- ❖ Mediante la investigación, evaluación y análisis de la situación actual de los procesos, recursos y requerimientos, se pudo evidenciar las vulnerabilidades encontradas en la seguridad física del área, operación y gestión de comunicación, entre ellas se pudo encontrar la falta de procedimientos, documentos, políticas para una buena centralización y gestión de la información.
- ❖ Siguiendo la norma de investigación con los objetivos establecidos se concluye la necesidad de la elaboración de un plan de Gestión para la seguridad de la Información basado en las normas ISO 27001, con el fin de disminuir los riesgos de la información institucional y académica.
- ❖ Gracias a la identificación de las vulnerabilidades de cada componente (Figura 15) dio la apertura a la estimación de riesgos por sus respectivos niveles como lo son: Crítico, Alto, Medio, Bajo, dando las bases para la mejora de los procesos en la Universidad Estatal de Milagro (Tabla 20).
- ❖ Los niveles de riesgos se determinaron mediante la probabilidad e impacto de las vulnerabilidades encontradas en cada una de los componentes (Tablas 14, 15, 16, 17, 18 y 19) los cuales están enlazados a robo, omisiones, ataques, fallos en los sistemas de gestión, accesos no autorizados.
- ❖ La Universidad Estatal de Milagro posee una infraestructura de red sólida, la cual soporta y evidencia una gran cantidad de estudiantes y empleados de la institución, sin embargo, una de las vulnerabilidades encontradas es, la falta de políticas, manuales y estandarización de la información y acceso físico al entorno o medio donde se puede obtener información crítica de la red.

4.2 Recomendaciones de mejora de la seguridad informática UNEMI

- ✓ De acuerdo a las evaluaciones realizadas de los riesgos y proporcionados por la norma ISO 27001, se recomienda la implementación de un plan de gestión de seguridad de la información lo antes posible para mitigar los riesgos que estén posiblemente expuestos los datos.
- ✓ Definición de las políticas de seguridad del sistema de gestión sistemas de información.
- ✓ Administración de activos, personal responsable, activos de la información.
- ✓ Comunicación y asignación de responsabilidades.
- ✓ Tener en cuenta la gestión de incidentes para la seguridad de la información, implementando procedimientos y responsabilidades para la gestión de eventos para la efectividad de tal.
- ✓ Implementación de una herramienta de detección de ataques a la red, para la toma de acciones preventivas y correctivas.
- ✓ Acoger las normativas ISO 27001 para la mejora de la seguridad informática.
- ✓ Definición de políticas de seguridad para el acceso físico a la data center.

BIBLIOGRAFÍA

- Arnold, M. & Osorio, F. (1998). Introducción a los Conceptos Básicos de la Teoría General de Sistemas. *Cinta de Moebio* (3), 1-12.
- Bertalanffy Von, L. (1976). *Teoría General de los Sistemas*. México: Editorial Fondo de Cultura Económica.
- Bracho-Ortega, C., Cuzme-Rodríguez, F., Pupiales-Yépez, C., Suárez-Zambrano, L., Peluffo-Ordóñez, D., & Moreira-Zambrano, C. (2017). Auditoría de seguridad informática siguiendo la metodología OSSTMMv3: caso de estudio. *Maskana*, 8, 307-319.
- Calvo, J., D. Parada & A. Flórez (2013). *Actualización del Modelo de Arquitectura de Seguridad de la Información - MASI v2.0*. Actas del VII Congreso Iberoamericano de Seguridad Informática CIBSI2013, 72-79, Ciudad de Panamá, Panamá
- Cando-Segovia, M.R. & Medina-Chicaiza, P. (2021). Prevención en ciberseguridad: enfocada a los procesos de infraestructura tecnológica. *Cuadernos de desarrollos aplicados a la TIC*, 10(1), 17-41. <https://doi.org/10.17993/3ctic.2021.101.17-41>
- Euroinnova (2019). *¿Qué es la teoría general de sistemas en informática?* Euroinnova Business School. Disponible en <https://www.euroinnova.edu.es/que-es-teoria-general-de-sistemas-en-informatica>
- Figuroa-Suárez, J. et al (2018). La seguridad informática y la seguridad de la información. *Polo del Conocimiento*, 2(2), 145-155 doi :<http://dx.doi.org/10.23857/pc.v2i12.420>
- Gantz J., Soper, P., Vavra, T., Lim, V., Smith, L., & Minton, S. (2015). El software sin licencia y las amenazas a la seguridad informática. International Data Corporation (IDC), 1-11
- Gil Vera, V. & Gil Vera, J. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. *Scientia Et Technica*, 22(2), 193-197
- Jaramillo, C., Jácome, L., Ordóñez, A., Gaona, M., Carrión, J. & Palma, M. (2017). Auditoría de gestión de seguridad informática, en entidades públicas y privadas en Loja. *MASKANA*, 8, 149-162
- Junco Romero, G. & Rabelo Padua, S. (2017). Consideraciones para mejorar la seguridad en los sistemas gestores de contenido (cms) Joomla. *Revista Cubana de Informática Médica*, 9(1), 88-95
- Maida, E. G., & Pacienza, J. (2015). Metodologías de desarrollo de software. *Pontificia Universidad Católica Argentina Santa María de los Buenos Aires*.
- Mendoza M. & Lorenzana P. (2013). Normatividad para las organizaciones: Políticas de seguridad de la información – Parte 1. *Revista Seguridad*. 16
- Miranda Cairo, M., Valdés Puga, O., Pérez Mallea, I., Portelles Cobas, R. & Sánchez

- Zequeira, R. (2016). Metodología para la implementación de la gestión automatizada de controles de seguridad informática. *Revista Cubana de Ciencias Informáticas* 10(10), 14-26
- Monasterio J. (2018). Un recorrido por la historia de los SI. Disponible en: <https://blogs.deusto.es/master-informatica/un-recorrido-por-la-historia-de-los-si/>
- Montesino, R., Baluja, W. & Porvén, J. (2013). Gestión automatizada e integrada de controles de seguridad informática. *RIELAC Revista de Ingeniería Electrónica, Automática y Comunicaciones*, 34, 40-58
- Muñoz, J. & Ponce, D. (2017). Metodología para seleccionar políticas de seguridad informática en un establecimiento de educación superior. *Maskana, Ciencias de la Computación. Congreso I+D+ingeniería*, 1-8
- Muñoz, M. & Rivas, L. (2015). Estado actual de equipos de respuesta a incidentes de seguridad informática. *RISTI Revista Ibérica de Sistemas e Tecnologias de Informação*, (03), 1-15. DOI: 10.17013/risti.e3.1-15
- Niño Benítez, Y. & Silega Martínez, N. (2018). Requisitos de Seguridad para aplicaciones web. *Revista Cubana de Ciencias Informáticas*, 12(No. Especial UCIENCIA), 205-221
- Parada, D., Flórez, A., & Gómez, U. (2018). Análisis de los Componentes de la Seguridad desde una Perspectiva Sistémica de la Dinámica de Sistemas. *Información tecnológica*, 29(1),27-38. <https://dx.doi.org/10.4067/S0718-07642018000100027>
- Patiño, S., Mosquera, C., Suárez, F. & Nevarez, R. (2017). Evaluación de seguridad informática basada en ICREA e ISO27001. *Universidad, Ciencia y Tecnología*, 21(85), 129-139
- Quiroz-Zambrano, S. & Macías-Valencia, D. (2017). Seguridad en informática: consideraciones. *Dominio de las Ciencias*, 3(5), 676-688
- Ramírez Castro, A., & Ortiz Bayona, Z. (2011). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. *Ingeniería*, 16(2), 56-66.
- Reyes Guerrero, D. (2017). *Análisis de riesgo de la información en la infraestructura tecnológica para el Gobierno Autónomo Descentralizado del Cantón Ventanas*. Universidad Técnica de Babahoyo.
- Rodríguez, A. (2020). Herramientas fundamentales para el hacking ético. *Revista Cubana de Informática Médica*, 12(1),116-131
- Rojas Valduciel, H. (2014). Elaboración de un plan de implementación de la ISO/IEC 27001: 2013. Trabajo Final de Máster. Universidad Politécnica de Cataluña
- Roque, R. & Juárez, C. Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios (2018). *Paakat: Revista de Tecnología y Sociedad*, 8(14), 1-13
- Sánchez. (2018). Responsabilidad: ¿Qué es? Concepto y claves para ser responsable.

Disponible en: <https://blog.cognifit.com/es/responsabilidad/>

Santiago, E., & Sánchez, J. (2017). Riesgos de ciberseguridad en las empresas. *Revista deCiencia, Tecnología y Medio Ambiente*, 15, 1-33.

Solarte, F., Enriquez, E. & Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica ESPOL – RTE*, 28(5), 492-507

Tecnología de Información (2018). Evolución de los Sistemas de Información. Disponible en <https://www.tecnologias-informacion.com/evolucionsistemas.html>

Voutssas, J. (2010). Preservación documental digital y seguridad informática. *Investigación Bibliotecológica*, 24(50), 127-155

ANEXO 1: Solicitud de ingreso a la Dirección TIC para el levantamiento de información.

Milagro, 05 de mayo de 2022

Estimada
Ing. Kerly Vanessa Palacios Zamora, Mgs.
Directora de Tecnología de la Información y Comunicaciones
Universidad Estatal de Milagro
Milagro. -

De mi consideración:

Yo, **LUIS ENRIQUE CASTILLO SALVATIERRA**, identificado con C.I. **0921071270**, ante usted respetuosamente me presento y expongo que:

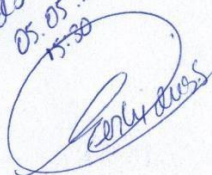
Actualmente me encuentro cursando una maestría en Tecnología de la Información, por lo cual solicito a usted de la manera más comedida se me permita realizar un TRABAJO DE TITULACIÓN bajo la modalidad de proyecto de investigación maestrante, con información correspondiente al área de Tecnología de la Información y Comunicaciones de la Universidad Estatal de Milagro, el mismo que consiste en: "Evaluación de la Seguridad Informática bajo las normas ISO/IEC 27001 en la Infraestructura Tecnológica de la Universidad Estatal de Milagro"

A tiempo de agradecerle la atención de la presente solicitud, aprovecho la oportunidad para reiterarle mi más alta consideración y estima.

Atentamente,



Ing. Luis Enrique Castillo Salvatierra
Estudiante de la Maestría en Tecnología de la Información
Universidad Estatal de Milagro

Recibido
05.05.2022
15:30


ANEXO 2: Solicitud de aceptación por la Dirección TIC para el levantamiento de información.

UNEMI
UNIVERSIDAD ESTATAL DE MILAGRO

Milagro, 09 de mayo de 2022

Estimado
Ing. Luis Enrique Castillo Salvatierra
Estudiante de la Maestría en Tecnología de la Información
Universidad Estatal de Milagro
Milagro. -

De mi consideración:

En atención a su solicitud emitida el 5 de mayo del 2022 con Nro. oficio S/N, en el que requiere se le permita realizar el TRABAJO DE TITULACIÓN en la Universidad Estatal de Milagro, bajo la modalidad de proyecto de investigación maestrante, el mismo que consiste en: "Evaluación de la Seguridad Informática bajo las normas ISO/IEC 27001 en la Infraestructura Tecnológica de la Universidad Estatal de Milagro"

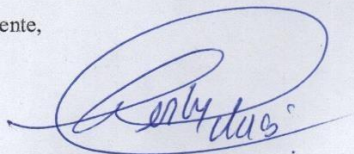
Al respecto, una vez analizada la viabilidad técnica de la petición realizada, se notifica que su solicitud ha sido APROBADA.

Ante lo expuesto, a partir de la presente fecha se puede acercarse hasta la Subdirección de Tecnologías de la Información y Comunicación de (TIC) Milagro, a realizar la investigación solicitada.

Particular que comunico a usted, para los fines consiguientes.

Con sentimientos de alta consideración y estima

Atentamente,



Ing. Kerly Vanessa Palacios Zamora
Directora de Tecnología de la Información y Comunicaciones

ANEXO 3: Aplicado al departamento tecnológico basado en la Norma ISO/IEC 27001.
 Aplicado y ponderado el checklist de acuerdo a la escala en el departamento de Tecnología de Información y Comunicación.

| Componente: INVENTARIO DE ACTIVO SG. NORMA ISO 27001 | | | | | | |
|--|-----------|-----------|------------|---------------------|--------------------|----------------------------|
| Objetivo/Ámbito: El presente checklist es con la finalidad de conocer y verificar el nivel de cumplimiento de procedimientos de control y mantenimiento de los bienes o activos tecnológicos de la institución. | | | | | | |
| ÁREA AUDITADA: | | | | | | |
| DEPARTAMENTO | | | | | | |
| TECNOLOGICO | | | | | | |
| PREGUNTAS: | SI | NO | N/A | CALIFICACION | PONDERACION | OBSERVACIONES |
| 1) ¿Posee con un Plan Estratégico? | | X | | 1 | NO cumple | |
| los inventario de los activos en formatos físicos? | | X | | 1 | NO cumple | |
| de los activos en formatos | | X | | 1 | NO cumple | |
| 3) Posee un control los inventario de los activos en formatos electrónicos? | | X | | 1 | NO cumple | |
| los inventarios de los activos de soporte de hardware? | | | | 3 | Cumple a medias | |
| a) Equipos Móviles (Smartphone, Tablet, celular, computadoras portátiles, etc.) | X | | | | | Se realiza con presupuesto |
| servidores, computadoras de escritorio, portátiles, etc.) | X | | | | | Se realiza con presupuesto |
| c) Periféricos de entrada (teclado, ratón, escáner, cámara digital, cámara web, etc.) | X | | | | | Se realiza con presupuesto |
| d) Periféricos de salida (monitor, audífonos, impresoras, proyector, etc.) | X | | | | | Se realiza con presupuesto |

| | | | | | | |
|--|---|---|--|--|--|--|
| dispositivos de almacenamiento (disco duro portátil, disco flexible, grabador de discos, CD, DVD, Blu-Ray, Memoria USB, etc.) | X | | | | | |
| Comunicaciones (Tarjetas USB y tarjeta PCMCIA para redes inalámbricas: WiFi, Bluetooth, GPRS, HSDPA; tarjeta USB para redes | X | | | | | |
| g) Tableros (de transferencia (bypass) de la unidad de energía (UPS); transferencia de salidas de energía, de transferencia automática de energía, etc.) | X | | | | | |
| acceso, de aire acondicionado, automático de extinción de incendios, | X | | | | | |
| los inventarios de los activos de soporte de software? | | X | | | | |
| a) Sistemas Operativos | | X | | | | |
| mantenimiento, administración de : servidores, sistema de redes de datos, sistemas de almacenamiento, telefonía, | | X | | | | |
| o software base (suite de ofimática, navegador de internet, mensajería instantánea, etc.) | | X | | | | |

| | | | | | | |
|--|---|---|--|--|---|---------------------|
| <p>6) ¿Posee control los inventarios de los activos de soporte de redes? Comunicaciones (Interfaces: RJ-45, RJ-11, etc.; Interfaz: RS232, USB, etc.; Panel de conexión, toma de red o puntos, b) Switches c) Router, Firewall, Controlador de red inalámbrica, etc. detección/prevenión de intrusos (IDS/IPS), firewall de aplicaciones web, etc. grupos de activos que no poseen custodios asignados?</p> | | | | | 1 | Compt/Sin custodios |
| | | X | | | | |
| | X | | | | | |
| | X | | | | | |
| | X | | | | | |
| | X | | | | 3 | Compt Custodios |

| Componente: SEGURIDAD DE LOS RECURSOS HUMANOS SG. NORMA ISO 27001 | | | | | | |
|--|----|----|-----|--------------|-------------|--------------------------------|
| Objetivo/Ámbito: El presente checklist es con la finalidad de conocer y verificar el nivel de cumplimiento de procedimientos de control y mantenimiento de los bienes o activos tecnológicos de la institución. | | | | | | |
| AREA AUDITADA: | | | | | | |
| Departamento Tecnológico | | | | | | |
| PREGUNTAS | SI | NO | N/A | CALIFICACION | PONDERACION | OBSERVACIONES |
| 1) ¿Se relacionan los procedimientos de mantenimiento correctivo, preventivo de los bienes: Software, Hardware y equipos de comunicación? | X | | | 3 | Cumple | |
| 2) ¿Se atribuye o notifica al personal del mal uso y destrucción de los equipos tecnológicos asignados? | X | | | 3 | Cumple | |
| 3) ¿El departamento de tecnología tiene restringido con claridad sus responsabilidades? | X | | | | | |
| 4) ¿Se posee objetivos para el departamento de tecnología? | | X | | 1 | No cumple | No existe un plan de seguridad |
| 5) ¿Posee definido por escrito los objetivos del departamento de tecnología? | | X | | 1 | No cumple | |

| | | | | | | | |
|--|---|---|--|--|---|------------------------|--|
| 6) ¿El personal que trabaja en el departamento de informática son los adecuados para cumplir las necesidades de este? | X | | | | 3 | cumple a medias | |
| 7) ¿El departamento tecnológico posee conflictos por la carga de trabajo? | | X | | | 1 | No cumple | No hay conflictos pero se van a ir que se acumulan |
| 8) ¿Bajo qué criterios existe la falta de cumplimiento de sus funciones? | | | | | 3 | Cumple sin incidencias | |
| a) falta de personal | X | | | | | | |
| b) Personal no capacitado | | | | | | | |
| c) carga de trabajo excesivas | | X | | | | | |
| c) por que realiza otras actividades | | X | | | | | |
| d) otras razones | | X | | | | | |
| 9) ¿Se efectúa la devolución de los equipos tecnológicos del personal que finaliza su contrato de trabajo por escrito? | X | | | | 3 | cumple sin incidencias | |

Componente: SEGURIDAD FISICA DEL ENTORNO SG. NORMA ISO 27001

Objetivo/Ámbito: El presente checklist es con la finalidad de conocer y verificar el nivel de cumplimiento de procedimientos de control y mantenimiento de los bienes o activos

| ÁREA AUDITADA: | | | | | | |
|--|----|----|-----|--------------|----------------------|---------------|
| Departamento Tecnológico | | | | | | |
| PREGUNTAS | SI | NO | N/A | CALIFICACION | PONDERACION | OBSERVACIONES |
| 1) ¿Se encuentran los repuestos y soportes de los equipos a una distancia prudente para evitar daños en caso de desastre de las instalaciones principales? | X | | | 2 | cumple sin evidencia | |
| 2) ¿Se ubica el equipo apropiado contra incendios? | X | | | 2 | cumple sin evidencia | |
| 3) ¿Se efectúan mantenimientos de las instalaciones eléctricas y ups? | X | | | 2 | cumple sin evidencia | |
| 4) ¿Se efectúan mantenimientos de los sistemas de climatización y ductos de ventilación? | X | | | 2 | cumple sin evidencia | |
| 5) ¿Se establecen controles para minimizar el riesgo de amenazas físicas, tales como robo, incendio, entre otras? | X | | | 2 | cumple sin evidencia | |
| 6) ¿Existen garantías físicas para trabajar en las áreas seguras? | X | | | 2 | cumple sin evidencia | |
| 7) ¿Los equipos se encuentran correctamente ubicados o protegidos de las amenazas o peligros del entorno? | X | | | 2 | cumple sin evidencia | |

| | | | | | | |
|--|---|--|--|---|----------------------|-----------------------------------|
| 8) ¿Se da seguimiento de las condiciones ambientales de humedad y temperatura? | X | | | 2 | Cumple sin evidencia | |
| 9) ¿Se posee protección contra variaciones de energía o descargas eléctricas en las edificaciones de la institución? | X | | | 2 | Cumple sin evidencia | |
| 10) ¿Se posee filtros protectores en las líneas de comunicación y en el suministro de energía? | X | | | 2 | Cumple sin evidencia | |
| 11) ¿Los equipos tecnológicos cuentan con protección contra fallas de suministro de energía? | X | | | 2 | Cumple sin evidencia | |
| 12) ¿Se garantiza el cableado de la red contra daño? | X | | | 2 | Cumple sin evidencia | |
| 13) ¿Se garantiza el cableado de energía de los cables de red? | X | | | 2 | Cumple sin evidencia | |
| 14) ¿Se separan los cables de energía de los cables de red según los estándares para el correcto funcionamiento de la red en el Data Center? | X | | | 2 | Cumple sin evidencia | |
| 15) ¿Se establecen las normativas locales e internacionales para la implementación de las redes? | X | | | 2 | Cumple sin evidencia | no tiene documentación respaldada |
| 16) ¿Se dispone de documentación, planos, diseños, de la distribución de todas conexiones de redes alámbricas e inalámbricas? | X | | | 2 | Cumple sin evidencia | |

| | | | | | |
|---|---|--|---|----------------------|---|
| 17) ¿Se posee un control de mantenimientos periódicos de los dispositivos tecnológicos y los equipos de acuerdo a las especificaciones y recomendaciones del proveedor? | X | | 1 | NO cumple | solo cuando es necesario |
| 18) ¿El personal calificado y autorizado realiza los mantenimientos de los equipos tecnológicos? | X | | 2 | cumple sin evidencia | |
| 19) ¿Se guardan registros de los mantenimientos correctivos, preventivos, fallas relevantes o sospechosas? | X | | 1 | NO cumple | |
| 20) ¿Se constituyen controles de mantenimientos programados? | X | | 1 | NO cumple | |
| 21) ¿Posee un registro de los mantenimientos correctivos y preventivos? | X | | 1 | NO cumple | |
| 22) ¿Posee custodia los equipos y medios que se encuentran fuera de la institución? | X | | 3 | cumple | El custodio es encargado de los equipos |
| 23) ¿Posee cobertura de seguro para proteger los equipos que se encuentran fuera de la institución? | X | | 1 | NO cumple | |
| 24) ¿Posee control de acceso para las redes inalámbricas del establecimiento? | X | | 2 | cumple sin evidencia | |
| 25) ¿Posee control de acceso a los servidores? | X | | 2 | cumple sin evidencia | |

Componente: GESTION DE COMUNICACION Y DE OPERACION SG. NORMA ISO 27001

Objetivo/Ámbito: El presente checklist es con la finalidad de conocer y verificar el nivel de cumplimiento de procedimientos de control y mantenimiento de los bienes o activos tecnológicos de la institución.

| ÁREA AUDITADA: | | | | | | |
|---|----|----|-----|--------------|-----------------------|---------------|
| Departamento Tecnológico | | | | | | |
| PREGUNTAS | SI | NO | N/A | CALIFICACION | PONDERACION | OBSERVACIONES |
| 1) ¿Posee documentación del proceso de respaldo y restauración de la información? | | X | | 1 | no cumple | |
| 2) ¿Posee documentación o instrucciones para el manejo de errores y otras condiciones que pueden surgir mediante ejecución de tareas? | | X | | 1 | no cumple | |
| 3) ¿Posee documentación de los procedimientos para el reinicio y recuperación del sistema en caso de fallas? | | X | | 1 | no cumple | |
| 4) ¿Posee programación del proceso de cambio con su prueba correspondiente? | | X | | 1 | no cumple | |
| 5) ¿Se delegan responsables de control de cambios en los equipos tecnológicos y software? | | X | | 1 | no cumple | |
| 6) ¿Se autorizan de manera formal los cambios o recomendaciones propuestas? | | X | | 1 | no cumple | |
| 7) ¿Posee distribución de responsabilidades y funciones en el Departamento Tecnológico? | X | | | 2 | cumple sin evidencias | |

| | | | | | | |
|---|---|---|--|---|-----------------------|---|
| 8) ¿Posee gestiones de escalabilidad para asegurar el desempeño requerido de los servicios y sistemas informáticos? | X | | | 2 | cumple sin evidencias | |
| 9) ¿Se prohíbe el uso de software no autorizado por la institución? | X | | | 2 | cumple sin evidencias | |
| 10) ¿Posee instalación y actualización automática de software de antivirus contra código malicioso? | X | | | 2 | cumple sin evidencias | |
| 11) ¿Se posee los sistemas operativos actualizados con las últimas versiones estable? | X | | | 2 | cumple sin evidencias | |
| 12) ¿Posee políticas de respaldo de la información antes del mantenimiento? | X | | | 1 | cumple | se realiza cumplimiento estándares NAW mandados |
| 13) ¿Separan el área de redes con el área de mantenimiento? | | X | | 2 | cumple sin evidencias | |
| 14) ¿Las áreas de redes y mantenimiento se encuentran separadas? | X | | | 2 | cumple sin evidencias | |
| 15) ¿Se realizan diseños antes de la implementación de una red? | X | | | 2 | cumple sin evidencias | |
| 16) ¿Denominan responsabilidades y procedimientos para la asistencia de equipos remotos? | X | | | 2 | cumple sin evidencias | |
| 17) ¿Realizan cambios de configuración de los controles de seguridad del sistema operativo? | X | | | 2 | cumple sin evidencias | |

Componente: CONTROL DE ACCESO SG. NORMA ISO 27001

Objetivo/Ámbito: El presente checklist es con la finalidad de conocer y verificar el nivel de cumplimiento de procedimientos de control y mantenimiento de los bienes o activos tecnológicos de la institución.

ÁREA AUDITADA:

Departamento Tecnológico

| PREGUNTAS | CALIFICACION | | | | OBSERVACIONES |
|---|--------------|----|-----|----|--------------------------------------|
| | SI | NO | N/A | ON | |
| 1) ¿Se documenta y encuentran identificados los equipos de las redes? | ✓ | | | 4 | si se identifica pero no hay control |
| 2) ¿Posee documentada la identificación de todos los equipos que permitidos de la red? | ✓ | | | 2 | hay algunos sin identificación |
| 3) ¿Se implementan procedimientos para controlar la instalación de software en sistemas operativos? | | ✓ | | 1 | no hay control |
| 4) ¿Posee un registro de las actualizaciones de software que se realizan, tipo auditoría | | ✓ | | 1 | no hay control |
| 5) ¿Se tienen restricciones de cambios de paquetes de software? | ✓ | | | 2 | hay algunos sin identificación |
| 6) 12. ¿Posee documentación del control de versiones para todas las actualizaciones de software? | ✓ | | | 1 | no hay control |

Componente: CUMPLIMIENTO SG. NORMA ISO 27001

Objetivo/Ámbito: El presente checklist es con la finalidad de conocer y verificar el nivel de cumplimiento de procedimientos de control y mantenimiento de los bienes o activos tecnológicos de la institución.

AREA AUDITADA:

Departamento
Tecnológico

| PREGUNTAS | SI | NO | N/A | CALIFICACION | PONDERACION | OBSERVACIONES |
|---|----|----|-----|--------------|-------------|---------------|
| 1) ¿Se posee inventario de todas las normas legales, estatutos y reglamentos pertinentes para cada programa de software, servicio informático e información que utilice el establecimiento? | | X | | 1 | no cumple | |
| 2) ¿Posee conocimiento de las leyes y normas generales relacionadas a la gestión de datos e información electrónica? | | X | | 1 | no cumple | |