UNIVERSIDAD NACIONAL DE CHIMBORAZO
FACULTAD DE INGENIERÍA
CARRERA DE INGENIERÍA DE TECNOLOGÍAS DE LA INFORMACIÓN

Auditoría informática de seguridad física en el área de redes en la Universidad Nacional de Chimborazo utilizando norma ISO 27001

Trabajo de Titulación para optar al título de Ingeniero en Tecnologías de la Información

Autor:
Tenorio Ordoñez Ivana Jolima

Tutor:
Ing. Fernando Molina. Ph.D.

Riobamba, Ecuador. 2024

DECLARATORIA DE AUTORÍA

Yo, Ivana Jolima Tenorio Ordoñez, con cédula de ciudadanía 0803589068, autor (a) (s) del trabajo de investigación titulado: Auditoría informática de seguridad física en el área de redes en la Universidad Nacional de Chimborazo utilizando norma ISO 27001, certifico que la producción, ideas, opiniones, criterios, contenidos y conclusiones expuestas son de mí exclusiva responsabilidad.

Asimismo, cedo a la Universidad Nacional de Chimborazo, en forma no exclusiva, los derechos para su uso, comunicación pública, distribución, divulgación y/o reproducción total o parcial, por medio físico o digital; en esta cesión se entiende que el cesionario no podrá obtener beneficios económicos. La posible reclamación de terceros respecto de los derechos de autor (a) de la obra referida, será de mi entera responsabilidad; librando a la Universidad Nacional de Chimborazo de posibles obligaciones.

En Riobamba, 13 de diciembre de 2024.

Ivana Jolima Tenorio Ordoñez

C.I: 0803589068

ACTA FAVORABLE - INFORME FINAL DEL TRABAJO DE INVESTIGACIÓN

En la Ciudad de Riobamba, a los 22 días del mes de octubre de 2024, luego de haber revisado el Informe Final del Trabajo de Investigación presentado por la estudiante **IVANA JOLIMA TENORIO ORDOÑEZ** con CC: **0803589068**, de la carrera **INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN** y dando cumplimiento a los criterios metodológicos exigidos, se emite el **ACTA FAVORABLE DEL INFORME FINAL DEL TRABAJO DE INVESTIGACIÓN** titulado **"AUDITORÍA INFORMÁTICA DE SEGURIDAD FÍSICA EN EL ÁREA DE REDES EN LA UNIVERSIDAD NACIONAL DE CHIMBORAZO UTILIZANDO NORMA ISO 27001"**, por lo tanto se autoriza la presentación del mismo para los trámites pertinentes.

Firmado electrónicamente por:
FERNANDO TIVERIO
MOLINA GRANJA

PhD. Fernando Molina Granja.

TUTOR

CERTIFICADO DE LOS MIEMBROS DEL TRIBUNAL

Quienes suscribimos, catedráticos designados Miembros del Tribunal de Grado para la evaluación del trabajo de investigación Auditoría informática de seguridad física en el área de redes en la Universidad Nacional de Chimborazo utilizando norma ISO 27001, presentado por Ivana Jolima Tenorio Ordoñez, con cédula de identidad número 0803589068, bajo la tutoría de Ph.D Fernando Tiverio Molina Granja; certificamos que recomendamos la APROBACIÓN de este con fines de titulación. Previamente se ha evaluado el trabajo de investigación y escuchada la sustentación por parte de su autor; no teniendo más nada que observar.

De conformidad a la normativa aplicable firmamos, en Riobamba 13 de diciembre de 2024.

Danny Velasco, Mgs.
PRESIDENTE DEL TRIBUNAL DE GRADO

Santiago Cisneros, Mgs.
MIEMBRO DEL TRIBUNAL DE GRADO

Gonzalo Allauca, Mgs.
MIEMBRO DEL TRIBUNAL DE GRADO

CERTIFICACIÓN

Que, **TENORIO ORDOÑEZ IVANA JOLIMA** con CC**: 0803589068**, estudiante de la Carrera **Ingeniería en Tecnologías de la Información**, Facultad de **INGENIERÍA;** ha trabajado bajo mi tutoría el trabajo de investigación titulado **"Auditoría informática de seguridad física en el área de redes en la Universidad Nacional de Chimborazo utilizando norma ISO 27001"**, cumple con el **8%**, de acuerdo al reporte del sistema Anti plagio **Turnitin**, porcentaje aceptado de **acuerdo** a la reglamentación institucional, por consiguiente autorizo continuar con el proceso.

Riobamba, 09 de diciembre de 2024

FERNANDO TIVERIO MOLINA GRANJA

PhD. Fernando Molina Granja
TUTOR

DEDICATORIA

El presente proyecto de investigación va dedicado a Dios, por ser mi guía, mi fortaleza y mi fuente de inspiración. Agradezco cada bendición y cada lección que he recibido en este camino.

A mis queridos padres, quienes con su amor incondicional y apoyo constante me han guiado a lo largo de este camino. Su fe en mí ha sido la fuerza que me ha impulsado a superar cada desafío.

A mi amado novio, por ser mi compañero de vida, mi fuente de inspiración y mi refugio en los momentos difíciles. Gracias por tu paciencia, tu comprensión y tu amor inagotable.

Con todo mi amor y gratitud.

Ivana Jolima Tenorio Ordoñez

AGRADECIMIENTO

Quiero expresar mi más sincero agradecimiento a la Universidad Nacional de Chimborazo por brindarme la oportunidad de realizar mis estudios en un entorno académico de excelencia.

A mi tutor, Ing. Fernando Molina, por su invaluable guía, apoyo y dedicación a lo largo de este proceso. Su orientación ha sido fundamental para el desarrollo de este trabajo.

Al Ing. Diego Reina, por sus enseñanzas, por compartir su conocimiento y experiencia, los cuales han sido esenciales para mi formación académica y profesional.

A los analistas de TIC's, por proporcionar la información necesaria y por su disposición para colaborar. Su ayuda ha sido crucial para la realización de este proyecto.

A todos ustedes, mi más profundo agradecimiento.

Ivana Jolima Tenorio Ordoñez

ÍNDICE GENERAL

DECLARATORIA DE AUTORÍA
DICTAMEN FAVORABLE DEL PROFESOR TUTOR
CERTIFICADO DE LOS MIEMBROS DEL TRIBUNAL
CERTIFICADO ANTIPLAGIO
DEDICATORIA
AGRADECIMIENTO
ÍNDICE GENERAL
ÍNDICE DE TABLAS
ÍNDICE DE FIGURAS
RESUMEN
ABSTRACT

CAPÍTULO I. INTRODUCCION 15

1.1 Planteamiento del Problema 15

1.2 Justificación 16

1.3 Problemática 16

1.4 Objetivos 17

1.4.1 General 17

1.4.2 Específicos 17

CAPÍTULO II. MARCO TEÓRICO 18

2.1 Seguridad de la Información: 18

2.1.1 Definición y conceptos básicos. 18

2.1.2 Importancia de la seguridad de la información en las organizaciones. 18

2.1.3 Principios fundamentales de la seguridad de la información. 19

2.2 Auditoría Informática: 20

2.2.1 Concepto y objetivos de la auditoría informática. 20

2.2.2 Tipos de auditoría informática. 21

2.2.3 Metodologías y técnicas de auditoría informática. 22

2.3 Norma ISO 27001: 23

2.3.1 Introducción a la norma ISO 27001. 23

2.3.2 Estructura y requisitos de la norma. 24

2.3.3 Proceso de implementación y certificación. 25

2.4 Seguridad Física:.....26

2.4.1 Definición y alcance de la seguridad física. 26

2.4.2 Importancia de la seguridad física en el ámbito de la seguridad de la información. ..27

2.4.3 Elementos y controles de seguridad física.....28

2.5 Redes de Computadoras: 28

2.5.1 Concepto y funcionamiento de las redes de computadoras. 28

2.5.2 Tipos de redes y sus características.....29

2.5.3 Vulnerabilidades comunes en las redes de computadoras.....29

2.6 Auditoría de Seguridad Física en Redes: 30

2.6.1 Concepto y objetivos de la auditoría de seguridad física en redes.....30

2.6.2 Metodologías y técnicas específicas para auditar la seguridad física en redes.....30

2.6.3 Herramientas utilizadas en la auditoría de seguridad física en redes. 31

CAPÍTULO III. METODOLOGIA 32

3.1 Metodología de Investigación.....32

3.2 Tipo de Investigación 32

3.3 Diseño de la Investigación.....32

3.4 Unidad de estudio.....32

3.5 Técnicas de Recolección de Datos.....32

3.6 Identificación de variables.....32

3.6.1 Variable dependiente 32

3.6.2 Variable independiente 33

3.7 Operacionalización de variables 34

3.8 Metodología de Desarrollo 36

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN 54

4.1. Resultados.....54

4.2. Discusión 60

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES 62

5.1. Conclusiones.....62

5.2. Recomendaciones.....63

BIBLIOGRÁFIA 64

ANEXOS.....67

ÍNDICE DE TABLAS

Tabla 1. Principios fundamentales 19
Tabla 2. Métodos y técnicas 22
Tabla 3. Elementos y Controles 28
Tabla 4. Herramientas 31
Tabla 5. Operacionalización de variables 34
Tabla 6. Planificación 39
Tabla 7. Asignación de tareas 40
Tabla 8. Switches piso 3 41
Tabla 9. Racks piso 3 42
Tabla 10. Access Point piso 3 42
Tabla 11. Patch Panel piso 3 42
Tabla 12. Switches piso 2 43
Tabla 13. Racks piso 2 43
Tabla 14. Access Point piso 2 44
Tabla 15. Patch Panel piso 2 44
Tabla 16. Switches piso 1 44
Tabla 17. Racks piso 1 45
Tabla 18. Access Point piso 1 45
Tabla 19. Patch Panels piso 1 45
Tabla 20. Evaluación de los switches del BLOQUE A según Anexo 4: 46
Tabla 21. Evaluación del cableado de red del BLOQUE A según Anexo 4: 46
Tabla 22. Evaluación de los racks del BLOQUE A según Anexo 4: 47
Tabla 23. Evaluación de los access point del BLOQUE A según Anexo 4: 47
Tabla 24. Evaluación de los patch panels del BLOQUE A según Anexo 4: 47
Tabla 25. Evaluación al personal 48
Tabla 26. Puntaje 48
Tabla 27. Evaluación del entorno del BLOQUE A según Anexo 4: 49
Tabla 28. Tareas y responsabilidades 56
Tabla 29. Cronograma 59

ÍNDICE DE FIGURAS

Ilustración 1. Principios de la norma 27001 24
Ilustración 2. Riesgos 56

RESUMEN

Este trabajo de tesis presenta una auditoría informática enfocada en la seguridad física de la red en el Edificio A de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo, utilizando como marco de referencia la norma ISO 27001. La investigación se centró en evaluar las medidas de seguridad existentes, identificar vulnerabilidades y proponer mejoras alineadas con estándares internacionales.

Inicialmente, se llevó a cabo una exhaustiva investigación sobre la norma ISO 27001, con énfasis en sus directrices para la seguridad física de la infraestructura de redes. Esta norma proporciona un marco sistemático para la gestión de la seguridad de la información, asegurando que se implementen controles adecuados para proteger los activos de información.

La auditoría incluyó la revisión de políticas de acceso, controles de vigilancia, y procedimientos de respuesta a incidentes. Se identificaron varios puntos críticos que necesitan mejoras para cumplir con los estándares de seguridad recomendados por la ISO 27001.

Basado en los hallazgos de la auditoría, se desarrolló un plan de contingencia que incluye recomendaciones específicas para mejorar la seguridad física, tales como la implementación de un sistema de control de acceso más robusto, auditorías periódicas de seguridad, y programas de capacitación para el personal. Estas medidas están diseñadas para mitigar riesgos, proteger los activos de información y asegurar la continuidad operativa.

El resultado de esta tesis proporciona un marco claro y aplicable para la gestión de la seguridad física de la red en la Universidad Nacional de Chimborazo, contribuyendo a una mayor protección de los recursos informáticos y cumplimiento con normas internacionales.

Palabras claves: Auditoría, seguridad física, red, ISO 27001

ABSTRACT

This thesis presents a computer audit focused on the physical network security of Building A at the Faculty of Engineering, Universidad Nacional de Chimborazo, using ISO 27001 as a framework. The research aimed to evaluate existing security measures, identify vulnerabilities, and propose improvements aligned with international standards.

Initially, an exhaustive study of ISO 27001 was conducted, emphasizing its guidelines for the physical security of network infrastructure. This standard provides a systematic framework for information security management, ensuring adequate controls are implemented to protect information assets.

The audit reviewed access policies, surveillance controls, and incident response procedures. Several critical areas needing improvement to meet ISO 27001 security standards were identified.

A contingency plan was developed based on audit findings with specific recommendations to enhance physical security, such as implementing a more robust access control system, conducting regular security audits, and initiating staff training programs. These measures are designed to mitigate risks, safeguard information assets, and ensure operational continuity.

The outcome of this thesis provides a clear and actionable framework for managing physical network security at Universidad Nacional de Chimborazo, contributing to enhanced protection of IT resources and compliance with international standards.

Keywords: Audit, physical security, network, ISO 27001

Reviewed by:
Ms.C. Ana Maldonado León
ENGLISH PROFESSOR
C.I.0601975980

CAPÍTULO I. INTRODUCCION

Se propone llevar a cabo una auditoría informática en la Facultad de Ingeniería de la Universidad Nacional de Chimborazo, centrándose en la seguridad física de las redes, siguiendo los estándares de la norma ISO 27001. En la era digital actual, donde la información es crucial, la seguridad informática se ha convertido en un componente vital para preservar la integridad, confidencialidad y disponibilidad de los datos.

El avance tecnológico y la creciente dependencia de las redes han incrementado las amenazas cibernéticas, convirtiendo la protección de la infraestructura de red en un desafío para la universidad. La diversidad de dispositivos y la sofisticación de los ataques resaltan la necesidad de reforzar la seguridad física en las redes para mitigar posibles incidentes como accesos no autorizados, interrupciones de servicios y robo de información sensible.

Preservar la confidencialidad de la información académica y administrativa es esencial para la continuidad de las operaciones universitarias, mientras que la integridad de los datos y la disponibilidad de los servicios son fundamentales para el funcionamiento eficiente de la institución. Aunque se han realizado esfuerzos para mejorar la seguridad informática, la eficacia de estas iniciativas debe evaluarse en el contexto específico de la universidad.

La propuesta de auditoría informática se motiva por el compromiso del autor con el fortalecimiento de la seguridad en entornos educativos, destacando la necesidad de una auditoría especializada que implemente la norma ISO 27001.

El objetivo de la investigación es llevar a cabo una auditoría informática exhaustiva en el área de redes, específicamente en la facultad de ingeniería ubicada en la Universidad Nacional de Chimborazo. Esto implica identificar vulnerabilidades, evaluar riesgos y proponer medidas concretas para fortalecer la infraestructura de red.

La propuesta se basa en un marco metodológico que incluye la revisión de políticas, la evaluación de infraestructura, el análisis de accesos no autorizados y la recomendación de mejores prácticas de seguridad. Al adoptar la norma ISO 27001, se busca un enfoque integral y sistemático, alineando las prácticas con estándares internacionales reconocidos.

1.1 Planteamiento del Problema

En la actualidad, la facultad de ingeniería de la Universidad Nacional de Chimborazo se enfrenta a desafíos significativos en la protección de su infraestructura de red, lo que ha generado la necesidad de una evaluación exhaustiva de la seguridad física en el área de redes. La falta de un análisis detallado de los riesgos específicos en este contexto universitario impide una comprensión completa de las amenazas y la implementación de medidas preventivas adecuadas. Esta necesidad se evidencia en estudios como el informe de ciberseguridad educativa de la Organización de Estados Americanos (OEA), que destaca la

importancia de abordar las vulnerabilidades específicas en las instituciones académicas para garantizar la continuidad de las operaciones y la protección de la información sensible.

El entorno universitario de la Universidad Nacional de Chimborazo se caracteriza por una red compleja y diversa, que conecta una variedad de dispositivos y sistemas críticos para el funcionamiento académico y administrativo. La creciente interconexión digital en el ámbito educativo expone a la facultad de ingeniería a amenazas como accesos no autorizados, interrupciones de servicios y posibles pérdidas de información confidencial. La necesidad de evaluar y fortalecer la seguridad física en el área de redes se convierte en un imperativo para preservar la integridad, confidencialidad y disponibilidad de los datos en este entorno dinámico.

1.2 Justificación

El planteamiento del problema se justifica en la complejidad de la infraestructura de red de la Universidad Nacional de Chimborazo, que conecta una variedad de dispositivos y sistemas críticos, aumentando la exposición a amenazas cibernéticas como accesos no autorizados e interrupciones de servicios. En este entorno, la protección de la información confidencial es fundamental para mantener la integridad, confidencialidad y disponibilidad de los datos sensibles, así como para garantizar la continuidad de las operaciones académicas y administrativas.

La aplicación de la norma ISO 27001 en la auditoría informática de la seguridad física en el área de redes se presenta como una estrategia clave, proporcionando un enfoque estructurado y sistemático para identificar, evaluar y tratar los riesgos de seguridad. Esto puede contribuir significativamente a fortalecer la seguridad de la infraestructura de red y mejorar los procesos de detección, respuesta y recuperación frente a incidentes de seguridad física.

Por lo tanto, el planteamiento del problema se fundamenta en la complejidad de la infraestructura de red, la importancia de proteger los datos sensibles, la relevancia de estándares internacionales, el impacto de las amenazas cibernéticas y la necesidad de una gestión efectiva de incidentes de seguridad física en la Facultad de Ingeniería de la Universidad Nacional de Chimborazo.

La presente intervención de auditoria se realizará en la Universidad Nacional de Chimborazo, campus Guano, Facultad de Ingeniería, bloque A.

1.3 Problemática

¿La aplicación de la norma ISO 27001 en la auditoría informática de la seguridad física en el área de redes de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo incidirá en la gestión de incidentes de seguridad física?

1.4 Objetivos

1.4.1 General

Desarrollar una auditoría informática de la seguridad física en el área de redes de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo.

1.4.2 Específicos

- Investigar la norma ISO 27001 enfocada en seguridad física de red.
- Realizar la auditoría informática de la seguridad física en el área de redes de la Universidad Nacional de Chimborazo, utilizando la norma ISO 27001.
- Elaborar un plan de contingencia para la gestión de seguridad física en área de redes Facultad de Ingeniería de la Universidad Nacional de Chimborazo.

CAPÍTULO II. MARCO TEÓRICO

2.1 Seguridad de la Información:

2.1.1 Definición y conceptos básicos.

El concepto de "Seguridad de la Información" se refiere a un conjunto de medidas, políticas y procedimientos diseñados para proteger la confidencialidad, integridad y disponibilidad de la información. En esencia, se trata de salvaguardar la información de cualquier tipo de amenaza o riesgo que pueda comprometer su valor, ya sea mediante accesos no autorizados, modificaciones no autorizadas, interrupciones en el servicio o cualquier otro tipo de incidente [1].

La seguridad de la información se basa en varios principios fundamentales, que incluyen:

- Confidencialidad: Garantizar que la información esté protegida contra accesos no autorizados. Esto se logra mediante la aplicación de controles de acceso, cifrado y políticas de privacidad [1].
- Integridad: Asegurar que la información sea precisa, completa y esté protegida contra modificaciones no autorizadas. Se implementa mediante la aplicación de controles de acceso, firmas digitales y registros de cambios [1].
- Disponibilidad: Asegurar que la información esté disponible y accesible cuando sea necesaria por parte de los usuarios autorizados. Se logra mediante la implementación de redundancia, planes de continuidad del negocio y medidas para prevenir interrupciones no planificadas [1].
- Autenticación: Verificar la identidad de usuarios y sistemas para garantizar que tengan los permisos adecuados para acceder a la información [1].
- Autorización: Otorgar permisos específicos a usuarios o sistemas una vez que se ha autenticado su identidad [1].
- Criptografía: Aplicar técnicas para asegurar la comunicación y el almacenamiento de información mediante algoritmos matemáticos que transforman los datos en formatos ilegibles para cualquier persona no autorizada [1].

2.1.2 Importancia de la seguridad de la información en las organizaciones.

La seguridad de la información es fundamental para las organizaciones en la era digital actual por muchas razones. En primer lugar, garantiza que los datos sensibles, como la información financiera, los datos personales de los clientes y los derechos de propiedad intelectual, estén protegidos contra el acceso no autorizado y, por tanto, contra el robo, la manipulación o la divulgación inadecuada [2].

Además, el cumplimiento de la legislación (como el GDPR de la UE o la HIPAA de EE. UU.) requiere fuertes medidas de seguridad para evitar sanciones legales y proteger la reputación de la organización. La seguridad de la información también juega un papel vital en el mantenimiento de la reputación de una organización. Las violaciones de seguridad pueden socavar la confianza de los clientes y socios comerciales, lo que resulta en una pérdida de ingresos y oportunidades comerciales.

También, la implementación de planes de continuidad del negocio y preparación para desastres garantiza que una organización pueda continuar operando incluso en condiciones adversas, contribuyendo a la estabilidad operativa y financiera [3].

Una sólida seguridad de la información puede crear un entorno que fomente la innovación y la competitividad. Cuando los empleados confían en que sus ideas y datos están protegidos, están más dispuestos a compartir información y colaborar en proyectos, lo que aumenta la productividad organizacional y la ventaja competitiva [4].

Por lo tanto, la seguridad de la información protege contra una variedad de amenazas cibernéticas, como malware, ransomware, phishing y ataques de denegación de servicio (DDoS), que pueden interrumpir las operaciones comerciales y causar pérdidas financieras significativas.

En resumen, la seguridad de la información es fundamental para proteger los activos críticos de una organización, cumplir con las leyes y regulaciones, mantener la reputación y garantizar la continuidad del negocio en un entorno digital cada vez más complejo y peligroso [5].

2.1.3 Principios fundamentales de la seguridad de la información.

Los principios fundamentales de la seguridad de la información son los pilares sobre los cuales se construye cualquier estrategia o programa de seguridad [6]. A continuación, la tabla 1 donde se especifican los principios más importantes:

Tabla 1. Principios fundamentales

Principios	Concepto
Confidencialidad	Este principio asegura que la información esté protegida contra accesos no autorizados. Se logra mediante la aplicación de controles de acceso, cifrado y políticas de privacidad.
Integridad	Garantiza que la información sea precisa, completa y esté protegida contra modificaciones no autorizadas. Se implementa mediante la aplicación de controles de acceso, firmas digitales y registros de cambios.
Disponibilidad	Asegura que la información esté disponible y accesible cuando sea necesaria por parte de los usuarios autorizados. Se logra mediante la implementación de redundancia, planes de continuidad del negocio y medidas para prevenir interrupciones no planificadas.
Autenticación	Verifica la identidad de usuarios y sistemas para garantizar que tengan los permisos adecuados para acceder a la información.
Autorización	Otorga permisos específicos a usuarios o sistemas una vez que se ha autenticado su identidad.
No repudio	Impide que una entidad niegue la autoría de una acción previamente realizada. Se logra mediante la implementación de registros y sistemas de auditoría.

Segregación de funciones	Divide las responsabilidades dentro de una organización para evitar conflictos de interés y reducir el riesgo de fraudes internos.
Principio de mínimo privilegio	Se basa en otorgar a los usuarios solo los permisos y accesos necesarios para realizar sus tareas, minimizando así la exposición a posibles riesgos de seguridad.
Evaluación y gestión de riesgos	Este principio implica identificar, evaluar y mitigar los riesgos potenciales para la seguridad de la información, con el objetivo de minimizar la probabilidad de incidentes de seguridad y sus impactos.

2.2 Auditoría Informática:

2.2.1 Concepto y objetivos de la auditoría informática.

La auditoría informática es un proceso independiente y objetivo que tiene como objetivo evaluar la eficacia, eficiencia y seguridad de los sistemas de información de una organización. Consiste en revisar y evaluar los controles, políticas, procedimientos y prácticas de seguridad informática para identificar posibles riesgos, deficiencias y áreas de mejora [7].

Los objetivos de la auditoría serían:
Evaluar el cumplimiento normativo: verificar que los sistemas de información y las prácticas de seguridad cumplan con las regulaciones, leyes y estándares relevantes como GDPR, HIPAA, ISO 27001, etc [8].

Identificar riesgos y vulnerabilidades: detectar posibles brechas de seguridad, brechas de control y posibles riesgos que podrían afectar la confidencialidad, integridad y disponibilidad de la información [8].

Mejorar los controles internos: evaluar la eficacia de los controles internos implementados para proteger los activos de información y garantizar la integridad de los datos [8].

Optimizar procesos y procedimientos: identificar oportunidades para mejorar procesos y procedimientos relacionados con la gestión de la información y la seguridad informática [8].

Evaluar efectividad y eficiencia: determinar si los recursos técnicos y humanos se están utilizando de manera efectiva y si las medidas de seguridad implementadas son efectivas para proteger los activos de la organización [8].

Garantice la confianza y la confiabilidad: proporcione a la gerencia y a las partes interesadas una evaluación independiente y objetiva de la seguridad y el cumplimiento de los sistemas de información [8].

Apoye la toma de decisiones: proporcione información y recomendaciones basadas en evidencia para ayudar a la gerencia a tomar decisiones informadas sobre la gestión de riesgos y la mejora continua de la ciberseguridad [8].

2.2.2 Tipos de auditoría informática.

La auditoría informática incluye varios tipos de auditorías que se utilizan para evaluar diversos aspectos de los sistemas de información y la seguridad informática de una organización [9]. A continuación, se detallan algunos de los tipos más comunes de auditorías informáticas:

- Auditoría de Seguridad Informática: Se enfoca en evaluar y verificar la efectividad de los controles de seguridad implementados en los sistemas de información para proteger la confidencialidad, integridad y disponibilidad de los datos. Esto puede incluir revisión de políticas de seguridad, control de acceso, gestión de parches, configuraciones de firewall, etc [10].

- Auditoría de Cumplimiento Normativo: Se centra en verificar que la organización cumple con las regulaciones, leyes y estándares relevantes en materia de seguridad de la información y protección de datos. Esto puede incluir el cumplimiento de legislaciones como GDPR, HIPAA, PCI DSS y estándares de seguridad como ISO 27001. Esto puede incluir revisar la arquitectura del sistema, la configuración del servidor, la administración de bases de datos y la protección de aplicaciones [10].

- Auditoría de Procesos de Negocio: Evaluar procesos y procedimientos relacionados con la gestión de la información y la seguridad informática en toda la organización. Esto puede incluir revisar políticas y procedimientos de seguridad, manejar incidentes de seguridad, procesos de respaldo y recuperación, etc [10].

- Auditoría forense informática: examen y recopilación de evidencia digital en caso de un incidente de seguridad como intrusión, fraude o actividad ilegal. Esto incluye analizar registros de actividad, sistemas de archivos, comunicaciones en línea y otros datos digitales para determinar la causa y el alcance del incidente [10].

- Auditoría de continuidad del negocio y recuperación ante desastres: evalúa la preparación y la capacidad de una organización para responder a las interrupciones del sistema de información y recuperarse de desastres. Esto puede incluir revisar los planes de continuidad del negocio, realizar copias de seguridad y restaurar datos y probar simulacros de desastre [10].

- Auditoría de seguridad física: Este tipo de auditoría se concentra en evaluar la seguridad de las instalaciones físicas de la organización, como edificios, centros de datos, almacenes y otros lugares donde se almacenan o procesan activos críticos. La auditoría de seguridad física puede abordar aspectos como el acceso físico a las

instalaciones, la vigilancia, los controles de entrada y salida, la protección contra intrusiones y la seguridad ambiental (por ejemplo, protección contra incendios, control de temperatura y humedad). Esta auditoría asegura que se implementen medidas adecuadas para proteger los activos físicos y reducir los riesgos de pérdida, robo o daño [10].

2.2.3 Metodologías y técnicas de auditoría informática.

Las auditorías informáticas utilizan diversos métodos y técnicas para garantizar una evaluación completa y eficaz de los sistemas de información y la seguridad informática de una organización [11]. A continuación, en la tabla 2 se presentan algunos de los métodos y técnicas más comunes:

Tabla 2. Métodos y técnicas

Métodos y técnicas	Concepto
COBIT (Objetivos de control para la información y tecnologías relacionadas)	Es un marco de gobierno y gestión de TI que proporciona un conjunto de principios, prácticas, herramientas y modelos para ayudar a las organizaciones a gestionar y controlar sus sistemas de información. En el contexto de las auditorías informáticas, COBIT se utiliza para definir estándares de control, identificar áreas de riesgo y evaluar la eficacia de los controles internos.
ISO/IEC 27001 (Sistemas de gestión de seguridad de la información)	Esta norma internacional especifica los requisitos para el establecimiento, implementación, mantenimiento y mejora de sistemas de gestión de seguridad de la información (SGSI) en las organizaciones. En la auditoría informática, se utiliza para evaluar el cumplimiento de los controles de seguridad de la información con los requisitos estándar.
ITIL (Biblioteca de infraestructura de tecnología de la información)	ITIL es un conjunto de mejores prácticas para la gestión de servicios de TI. En el contexto de la auditoría de TI, ITIL se utiliza para evaluar la eficacia de los procesos y procedimientos relacionados con la gestión de servicios de TI, como la gestión de incidentes, la gestión de cambios y la gestión de problemas.
Herramientas de evaluación y escaneo de vulnerabilidades	Estas herramientas se utilizan para identificar y evaluar vulnerabilidades en sistemas, redes y aplicaciones de información. Analizan de forma proactiva los sistemas en busca de vulnerabilidades de seguridad, como puertos abiertos, configuraciones incorrectas y software desactualizado o que no se carga.
Análisis de registros y registros de auditoría	El análisis de registros y registros de auditoría es una técnica utilizada para revisar y analizar archivos de registro generados por sistemas de información, aplicaciones y dispositivos de red. Esto puede incluir registros de eventos, registros de acceso, registros de cambios y otros registros relevantes para identificar actividades sospechosas, patrones de uso inusuales y posibles violaciones de seguridad

Entrevistas y encuestas	Las entrevistas y encuestas se utilizan para recopilar información sobre los procesos, procedimientos y controles de seguridad de una organización. Los auditores pueden entrevistar a empleados clave y administradores de sistemas para obtener información sobre prácticas, funciones y responsabilidades de seguridad

2.3 Norma ISO 27001:

2.3.1 Introducción a la norma ISO 27001.

ISO 27001 es un estándar internacional de gestión de seguridad de la información que proporciona un marco integral para establecer, implementar, mantener y mejorar sistemas de gestión de seguridad de la información (SGSI) dentro de una organización [12]. La siguiente es una introducción a ISO 27001:

La norma ISO 27001, titulada "Tecnología de la información - Tecnología de seguridad - Sistemas de gestión de seguridad de la información - Requisitos", define los requisitos y las mejores prácticas para el establecimiento de un SGSI eficaz en una organización. Fue desarrollado por la Organización Internacional de Normalización (ISO) y se basa en un enfoque de ciclo de vida continuo para la gestión de la seguridad de la información.

El principal objetivo de ISO 27001 es proporcionar un sistema sistemático y proactivo para identificar, gestionar y reducir los riesgos de seguridad de la información, garantizando así la confidencialidad, integridad y disponibilidad de la información crítica de una organización [13].

Aspectos clave de ISO 27001 incluyen:

Enfoque basado en riesgos: el estándar utiliza un enfoque basado en riesgos para la gestión de la seguridad de la información, lo que significa que las organizaciones deben identificar y evaluar los riesgos de seguridad de la información y tomar medidas para mitigarlos de acuerdo con su impacto y probabilidad de ocurrencia [14].

Requisitos del sistema de gestión: Define el conjunto de requisitos que una organización debe cumplir para implementar y mantener un SGSI eficaz. Esto incluye establecer políticas de seguridad de la información, identificar activos de información, evaluar riesgos, implementar controles de seguridad y revisarlos periódicamente y mejorarlos continuamente [14].

Enfoque de mejora continua: ISO 27001 promueve un enfoque de mejora continua de la seguridad de la información, lo que significa que las organizaciones deben revisar periódicamente su SGSI, identificar áreas de mejora y tomar medidas para fortalecer su postura de seguridad [14].

Ilustración 1. Principios de la norma 27001

Fuente: [11]

2.3.2 Estructura y requisitos de la norma.

La norma ISO 27001 sigue una estructura clara, detallada y define los requisitos para el establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información (SGSI) eficaz en una organización [15]. La estructura estándar y los principales requisitos se describen a continuación:

- Alcance del SGSI: La organización debe definir el alcance del SGSI y definir los límites y áreas que cubrirá el sistema de gestión de seguridad de la información. Estrategia de seguridad de la información: la organización debe desarrollar una estrategia de seguridad de la información que defina los objetivos generales y el compromiso de la alta dirección para garantizar la seguridad de la información [16].

- Planificación del SGSI: Los objetivos de seguridad de la información y el proceso de identificación y evaluación de los riesgos de seguridad deben determinarse a la luz de los requisitos legales, reglamentarios y contractuales aplicables [15].

- Apoyo a la gestión: la alta dirección debe demostrar liderazgo y compromiso con la seguridad de la información y asignar responsabilidades y recursos adecuados al SGSI [16].

- Recursos humanos, técnicos y financieros: Se deben asignar los recursos humanos, técnicos y financieros necesarios para implementar y mantener eficazmente el SGSI [16]. Gestión de riesgos: las organizaciones deben utilizar un enfoque basado en riesgos para identificar, evaluar y abordar de forma sistemática y documentada los riesgos de seguridad de la información [16].
- Control de riesgos: Se deben implementar medidas de control de seguridad de la información para mitigar los riesgos identificados y se deben seleccionar con base en los resultados de un análisis de riesgos, teniendo en cuenta los controles definidos en la norma ISO/IEC 27002 [16].

- Evaluación del desempeño: La organización monitorea, mide, analiza y evalúa periódicamente el desempeño del SGSI a través de indicadores clave de desempeño y auditorías internas [16].

- Mejora Continua: Se deben tomar acciones para mejorar continuamente el SGSI en función de los resultados de la evaluación del desempeño, las revisiones de la gestión y las oportunidades de mejora identificadas. La estructura y los requisitos de ISO 27001 están diseñados para proporcionar un marco integral y sistemático para la gestión de la seguridad de la información dentro de una organización que garantice la confidencialidad, integridad y disponibilidad de la información y los activos críticos [16].

2.3.3 Proceso de implementación y certificación.

La implementación y certificación de la norma ISO 27001 implica un proceso estructurado que requiere la participación de toda la organización [17]. El proceso general de implementación y certificación se describe a continuación:

- Comprender los requisitos: el primer paso es comprender los requisitos de la norma ISO 27001 y cómo se aplican a la organización. Esto incluye revisar estándares, identificar requisitos específicos y cómo deben cumplirse [18].

- Compromiso de la dirección: la alta dirección debe demostrar su compromiso con la seguridad de la información y apoyar la implementación de un Sistema de gestión de seguridad de la información (SGSI) proporcionando recursos y liderazgo adecuados [18].

- Educación y concientización: Se debe brindar educación y concientización sobre seguridad de la información a todos los empleados para garantizar que comprendan los riesgos y responsabilidades asociados con la seguridad de la información [18].

- Análisis de riesgos: se debe realizar un análisis de riesgos para identificar y evaluar los riesgos de seguridad de la información que enfrenta la organización. Esto incluye identificar activos de información, evaluar amenazas y vulnerabilidades y determinar el impacto y la probabilidad de que ocurra el riesgo [18].

- Selección de medios de control: Los controles de seguridad de la información deben seleccionarse y documentarse para mitigar los riesgos identificados. Esto incluye revisar los controles definidos en la norma ISO/IEC 27002 y seleccionar controles que sean aplicables y proporcionales a los riesgos identificados [18].

- Implementación de controles: Se deben implementar controles seleccionados, que pueden incluir cambios en los procesos, procedimientos, tecnología y prácticas de gestión de la organización [18].

- Documentación SGSI: El sistema de gestión de seguridad de la información (SGSI) debe estar documentado de acuerdo con los requisitos de la norma ISO 27001, incluidas políticas de seguridad de la información, procedimientos operativos, registros y evidencia. Áreas para mejorar. Esto incluye revisar la documentación del SGSI, realizar entrevistas y revisar la implementación de controles [18].

- Certificación: una vez que se haya implementado el SGSI y se hayan completado las auditorías internas satisfactorias, la organización puede solicitar la certificación ISO 27001 a través de un organismo de certificación externo. La empresa realizará una auditoría de certificación para verificar el cumplimiento de los requisitos de la norma [18].

- Mantenimiento y Mejora Continua: Después de la certificación, la organización debe continuar manteniendo y mejorando el SGSI a través de revisiones periódicas, evaluaciones de desempeño y acciones correctivas y preventivas [18].

- El proceso de implementación y certificación ISO 27001 es un proceso continuo que requiere compromiso organizacional, recursos y esfuerzos continuos, pero proporciona beneficios significativos en la protección de la información y la mejora de la seguridad organizacional [16].

2.4 Seguridad Física:

2.4.1 Definición y alcance de la seguridad física.

La seguridad física se refiere a medidas y controles diseñados para proteger los activos, recursos y personas de una organización de amenazas físicas como robo, vandalismo, intrusión, desastres naturales y otros eventos que pueden causar daños o pérdidas. El campo de la seguridad física incluye todos los aspectos relacionados con la protección de las instalaciones, la infraestructura y el personal de una organización [19].

La seguridad física incluye varios elementos clave para proteger las instalaciones, los activos y el personal de una organización de amenazas físicas. Esto incluye implementar controles de acceso físico como cerraduras, tarjetas de acceso, sistemas de control de acceso biométrico y videovigilancia para evitar el acceso no autorizado a las instalaciones.

Además, la seguridad perimetral incluye proteger el perímetro físico de la propiedad con vallas, muros, barreras para vehículos y sistemas de detección de intrusos para ayudar a prevenir intrusiones no deseadas [20].

La protección de los activos físicos es otro fundamento y se refiere a la seguridad de los equipos, el inventario, las materias primas y los recursos críticos de una organización. Esto se logra mediante la implementación de medidas como candados, cables de seguridad, etiquetas de activos y sistemas de seguimiento de activos. La seguridad ambiental es esencial para proteger los activos de peligros como incendios, inundaciones y terremotos a través de sistemas de detección y extinción de incendios, alerta temprana y planes de respuesta a emergencias [21].

La protección de las personas es otra prioridad con medidas que incluyen la instalación de sistemas de alarma de emergencia, iluminación adecuada, formación en seguridad y procedimientos de evacuación. También, el control de acceso de vehículos es importante para evitar que vehículos no autorizados entren en las instalaciones mediante la implementación de controles como barreras de acceso, puertas automáticas, sistemas de reconocimiento de matrículas y control de acceso remoto.

Podemos decir que, la seguridad física incluye todas las medidas y controles diseñados para garantizar que el entorno operativo de una organización sea seguro protegiendo sus instalaciones, activos y personal de amenazas físicas [10].

2.4.2 Importancia de la seguridad física en el ámbito de la seguridad de la información.

La seguridad física juega un papel importante en la seguridad de la información al proteger los activos físicos que almacenan, procesan y transmiten datos importantes para la organización. Su importancia se refleja en varios aspectos clave. En primer lugar, reducir significativamente el riesgo de acceso no autorizado a la infraestructura de TI y a los datos confidenciales mediante la implementación de medidas como cerraduras de puertas, sistemas de control de acceso y videovigilancia para controlar el acceso a áreas críticas [22].

Además, la seguridad física ayuda a prevenir robos, vandalismo y vandalismo, reduciendo el riesgo de pérdida de datos y tiempo de inactividad. Esto es especialmente cierto para el cumplimiento legal, ya que muchas regulaciones y estándares de seguridad requieren controles físicos para proteger los activos de información y garantizar el cumplimiento legal.

Además, la seguridad física respalda y complementa los controles de seguridad lógicos, como los firewalls y el cifrado, para garantizar la eficacia de estos controles en la protección de la infraestructura que los respalda [22].

También elimina los riesgos asociados con desastres naturales y fallas de hardware, y garantiza la disponibilidad e integridad de los datos en caso de eventos imprevistos. En resumen, la seguridad física es la base de la seguridad de la información. Garantiza la

integridad, confidencialidad y disponibilidad de los datos clave de una organización. Su correcta implementación es fundamental para la protección integral de los activos de información [12].

2.4.3 Elementos y controles de seguridad física.

La seguridad física consta de varios elementos y controles diseñados para proteger las instalaciones, los activos y el personal de una organización de amenazas físicas [23]. A continuación, en la tabla 3 se presentan los aspectos más destacados y controles:

Tabla 3. Elementos y Controles

Elementos y Controles	Concepto
Control de Acceso Físico	Cerraduras Tarjetas de Acceso Sistemas de Control de Acceso Biométrico Vigilancia por Video
Seguridad Perimetral	Cercas Muros Barreras Vehiculares Sistemas de Detección de Intrusos
Vigilancia y Monitoreo	Vigilancia por Video Sistemas de Monitoreo
Protección contra Desastres	Sistemas de Detección y Extinción de Incendios Sistemas de Alerta Temprana Planes de Respuesta a Emergencias
Controles de Acceso de Vehículos	Barreras de Entrada Puertas Automáticas Sistemas de Reconocimiento de Placas

Fuente: [23]

2.5 Redes de Computadoras:

2.5.1 Concepto y funcionamiento de las redes de computadoras.

Las redes de computadoras son sistemas que permiten la comunicación y el intercambio de información entre dispositivos conectados, como computadoras, servidores y dispositivos móviles. Funcionan mediante la transmisión de datos a través de medios de comunicación, como cables de red o conexiones inalámbricas, utilizando protocolos de comunicación estándar. Esto facilita el acceso compartido a recursos, como archivos y aplicaciones, y permite la colaboración y el intercambio de datos entre usuarios y sistemas en una amplia variedad de entornos, desde entornos domésticos hasta entornos empresariales [24].

2.5.2 Tipos de redes y sus características.

- LAN (Red de Área Local): Limitada a un área geográfica pequeña, como una oficina o un edificio. Alta velocidad y bajo costo de implementación [25].

- WAN (Red de Área Amplia): Extiende su alcance sobre áreas geográficas más grandes, como ciudades o países. Utiliza servicios de telecomunicaciones y suele ser más lenta que una LAN [25].

- MAN (Red de Área Metropolitana): Cubre una ciudad o una región metropolitana. Ofrece una velocidad y capacidad intermedias entre LAN y WAN [25].

- Redes Inalámbricas: Utilizan tecnologías como Wi-Fi para la comunicación sin cables. Ofrecen movilidad y flexibilidad, pero pueden ser más vulnerables a intrusiones [25].

- Redes de Malla: Cada dispositivo se conecta con múltiples nodos, lo que proporciona redundancia y fiabilidad. Son utilizadas en aplicaciones críticas donde la disponibilidad es fundamental [25].

2.5.3 Vulnerabilidades comunes en las redes de computadoras.

- Falta de actualizaciones de seguridad: No aplicar parches y actualizaciones puede dejar sistemas vulnerables a exploits conocidos [26].

- Contraseñas débiles: Contraseñas fáciles de adivinar o predeterminadas pueden ser fácilmente comprometidas por atacantes [26].

- Ataques de ingeniería social: Los usuarios pueden ser engañados para revelar información confidencial o realizar acciones que comprometan la seguridad de la red [26].

- Malware y ataques de phishing: Descargas de archivos infectados o hacer clic en enlaces maliciosos pueden infectar dispositivos con malware o comprometer credenciales de usuario [26].

- Falta de cifrado: Las comunicaciones no cifradas pueden ser interceptadas y los datos sensibles expuestos [26].

- Configuraciones inseguras de dispositivos de red: Configuraciones predeterminadas o mal configuradas pueden dejar puertas traseras abiertas para atacantes [26].

2.6 Auditoría de Seguridad Física en Redes:

2.6.1 Concepto y objetivos de la auditoría de seguridad física en redes.

Las auditorías de seguridad de la red física son fundamentales para evaluar y validar los controles implementados en la infraestructura física de una red informática. Se centra en identificar vulnerabilidades potenciales, evaluar la eficacia de los mecanismos de control existentes y garantizar el cumplimiento de las políticas y estándares de seguridad establecidos.

Esta auditoría contribuye en gran medida a fortalecer la seguridad general de una organización al identificar y abordar debilidades como el acceso no autorizado y las brechas de protección ante desastres [27].

Los objetivos principales de una auditoría de seguridad de la estructura cibernética son la mitigación de riesgos, el cumplimiento normativo y garantizar la integridad y disponibilidad de los recursos de la red.

Al evaluar la resiliencia de la red y su resiliencia frente a amenazas físicas como incendios o daños, así como revisar otras medidas como la prevención de intrusiones y la seguridad ambiental, esta auditoría se convierte en un componente clave de la protección integral de la infraestructura de la red [28].

2.6.2 Metodologías y técnicas específicas para auditar la seguridad física en redes.

Para realizar auditorías de seguridad física de las redes de manera efectiva, una evaluación integral de la protección de la infraestructura física requiere una serie de métodos y tecnologías específicos. Estos métodos incluyen una revisión detallada de los controles de acceso físico implementados (como cerraduras, sistemas de control de acceso y videovigilancia) para verificar su correcto funcionamiento y configuración.

Además, se realiza un escaneo de vulnerabilidades para identificar posibles debilidades de seguridad física de la red, incluidas búsquedas de vulnerabilidades de defensa perimetral, fallas del sistema de detección de intrusiones y brechas de protección ante desastres [29].

Otra técnica ampliamente utilizada son las pruebas de penetración física, que implican simular un ataque del mundo real para evaluar la resistencia de los controles de seguridad física y determinar su eficacia para prevenir y detectar intrusiones. Estas pruebas pueden incluir intentos de obtener acceso no autorizado a áreas restringidas, alterar el equipo de seguridad y evaluar la capacidad de responder a situaciones de emergencia.

Además, se evalúan medidas de seguridad ambiental (como protección contra incendios, inundaciones y otros desastres naturales) para garantizar la integridad y disponibilidad de los recursos de la red contra amenazas físicas externas [29].

2.6.3 Herramientas utilizadas en la auditoría de seguridad física en redes.

Una auditoría de seguridad de la red física implica evaluar los controles y medidas de seguridad implementadas para proteger la infraestructura física de la red informática. Existe una variedad de herramientas especializadas para realizar esta evaluación, incluidos escáneres de puertos, herramientas de análisis de tráfico, sistemas de pruebas de penetración y sistemas de videovigilancia [30].

A continuación, en la tabla 4 se presentan estas herramientas que permiten identificar vulnerabilidades, detectar anomalías y garantizar la integridad y disponibilidad de los recursos de la red frente a amenazas físicas:

Tabla 4. Herramientas

Herramientas	Descripción
Nmap	Escáner de puertos y mapeo de redes para identificar dispositivos activos y servicios en una red.
Wireshark	Herramienta de análisis de tráfico de red que permite inspeccionar paquetes y detectar anomalías.
Metasploit	Marco de pruebas de penetración que incluye módulos para realizar pruebas de seguridad física en redes.
Nessus	Escáner de vulnerabilidades que puede identificar posibles puntos débiles en la seguridad física.
CCTV (Circuito Cerrado de Televisión)	Sistemas de videovigilancia para monitorear y grabar actividades en áreas críticas de la red.

Fuente: [30]

CAPÍTULO III. METODOLOGIA

3.1 Metodología de Investigación

Para llevar a cabo la auditoría informática de seguridad física en el área de redes en la facultad de ingeniería de la Universidad Nacional de Chimborazo utilizando la norma ISO 27001, se siguió una metodología mixta que combina elementos cualitativos y cuantitativos. Esto permitió obtener una visión holística de la situación de seguridad física en el área de redes de la facultad.

3.2 Tipo de Investigación

La investigación fue de tipo exploratoria y descriptiva. La parte exploratoria se enfocó en comprender en profundidad la infraestructura de redes y los sistemas de seguridad física existentes en la facultad de ingeniería de Universidad Nacional de Chimborazo. Por otro lado, la parte descriptiva se centró en identificar y documentar los hallazgos de la auditoría de acuerdo con los estándares establecidos por la norma ISO 27001.

3.3 Diseño de la Investigación

El diseño de la investigación fue no experimental y transversal. Se recopilaron datos en un momento específico para evaluar el estado actual de la seguridad física en el área de redes de la facultad de ingeniería. Además, se utilizó un enfoque cualitativo para analizar los procedimientos y controles de seguridad existentes, así como un enfoque cuantitativo para medir la eficacia y el cumplimiento de las medidas de seguridad.

3.4 Unidad de estudio

La unidad de estudio para esta investigación es el Bloque A de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo. Se examinarán todos los activos de información y sistemas relacionados con el área de redes de este bloque para evaluar la seguridad física de manera integral.

3.5 Técnicas de Recolección de Datos

Para la recopilación de los requerimientos de la auditoría a desarrollar se utilizó la técnica de la entrevista con observaciones, entrevistas, cuestionarios.

3.6 Identificación de variables

3.6.1 Variable dependiente

Norma ISO 27001

3.6.2 Variable independiente

Gestión de la seguridad física en área de redes Facultad de Ingeniería de la Universidad Nacional de Chimborazo.

3.7 Operacionalización de variables

A continuación, en la tabla 5, podremos observar la operacionalización de variables:

Tabla 5. Operacionalización de variables

PROBLEMA	TEMA	OBJETIVOS	VARIABLES	CONCEPTUALIZACION	DIMENSION	INDICADORES
¿La aplicación de la norma ISO 27001 en la auditoría informática de la seguridad física en el área de redes de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo incidirá en la gestión de incidentes de seguridad física?	Auditoría informática de seguridad física en el área de redes en la Universidad Nacional de Chimborazo utilizando norma ISO 27001	**General** • Desarrollar una auditoría informática de la seguridad física en el área de redes de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo.	**Independiente** Norma ISO 27001	Es un estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI).	Desarrollo de la auditoría informática de la seguridad física en el área de redes en la Universidad Nacional de Chimborazo.	- Probabilidad de implementación - Percepción de la efectividad de las medidas - Resiliencia ante amenazas físicas
		Específicos • Investigar la norma ISO 27001 enfocada en seguridad física de red. • Realizar la auditoría informática de la seguridad física en el área de redes de la Universidad Nacional de Chimborazo,	**Dependiente** Gestión de la seguridad física en área de redes Facultad de Ingeniería de la Universidad Nacional de Chimborazo.	Es la medida de protección contra amenazas físicas, como accesos no autorizados o daños, aplicada a los componentes de la red.	Gestión de la seguridad física	- Numero de cumplimiento de normativas - Numero de Índice de incidentes - Tiempo de respuesta ante incidentes físicos

	utilizando la norma ISO 27001. • Elaborar un plan de contingencia para la gestión de seguridad física en área de redes Facultad de Ingeniería de la Universidad Nacional de Chimborazo.	

3.8 Metodología de Desarrollo

El Project Management Institute (PMI) creó una guía llamada PMBOK, que estandariza las prácticas y procesos de gestión de proyectos. La siguiente guía está organizada en cinco fases o grupos de procedimientos fundamentales:

Iniciación: el proyecto o una fase de este se define y autoriza. Se identifican los objetivos, se crean los documentos preliminares del proyecto, como el acta de constitución, y se asignan los primeros recursos.

Planificación: aquí se establece el alcance del proyecto, se definen sus objetivos detallados y se crea un plan de gestión. La creación de planes subsidiarios para la gestión del alcance, el cronograma, los costos, la calidad, los recursos humanos, las comunicaciones, los riesgos y las adquisiciones es parte de esto.

Ejecución: En esta fase, se realizan las tareas especificadas en el plan de gestión del proyecto para cumplir con los requisitos del proyecto. Esto implica la coordinación de personas y recursos, la gestión de las expectativas de las partes interesadas y la garantía de la calidad del trabajo.

Monitoreo y Control: Durante esta etapa, se monitorea, analiza y controla el progreso y el desempeño del proyecto. Se identifican y gestionan los cambios necesarios, se garantizan las correcciones necesarias y se cumplen los objetivos del proyecto.

Cierre: Esta etapa implica la finalización oficial de todas las actividades o una fase del proyecto. Se asegura de que todos los entregables se hayan completado y que el cliente los acepte. Se cierran los contratos, se liberan los recursos del proyecto y se registran las enseñanzas aprendidas.

FASE DE INICIACIÓN

Objetivo: definir y autorizar el proyecto o una fase de este. Durante esta fase, se identifican los objetivos y el alcance inicial del proyecto, se desarrollan los documentos preliminares, como el acta de constitución del proyecto, y se asignan los recursos iniciales necesarios para comenzar. Esto establece una base clara y autorizada para el desarrollo del proyecto.

Propósito del proyecto:

Realizar una auditoría de seguridad física computarizada en el área de redes de la Facultad Técnica de la Universidad Nacional de Chimborazo utilizando como sistema de referencia la norma ISO 27001.

Justificación del proyecto:

La auditoría informática de seguridad física realizada en el área de redes de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo se fundamenta en la necesidad general de garantizar la integridad, confidencialidad y disponibilidad de la información crítica almacenada y procesada en sistemas seguros.

En un entorno cada vez más dependiente de la tecnología y constantemente expuesto a riesgos cibernéticos, se deben tomar medidas proactivas para proteger los activos digitales de la facultad de posibles amenazas, ataques maliciosos o incidentes de seguridad.

Además, como institución académica líder, la Universidad Nacional de Chimborazo está comprometida con los más altos estándares de seguridad de la información para proteger los datos confidenciales de estudiantes, profesores y administradores mientras mantiene su reputación y credibilidad en la comunidad para la comunidad.

Por lo tanto, la auditoría informática con el estándar ISO 27001 identificará vulnerabilidades físicas en la red, evaluará el cumplimiento de los controles de seguridad existentes y dará recomendaciones para posibles mejoras de la seguridad de la información de la facultad. Esta medida fortalecerá significativamente la postura de seguridad de la agencia, brindará confianza y tranquilidad a todas las partes interesadas.

Estudio de factibilidad:

1. Metas del Proyecto:

El objetivo principal del proyecto es realizar una auditoría informática de seguridad física en el área de redes de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo, utilizando el marco de referencia de la norma ISO 27001.

Las metas específicas incluyen:

- Realizar una evaluación de la seguridad física de la infraestructura de la red.
- Identificar vulnerabilidades potenciales y amenazas de seguridad.
- Verificar que se cumplan las normas y procedimientos de seguridad.
- Hacer recomendaciones sobre cómo mejorar la seguridad de la red.

Cronograma:

El cronograma tentativo de ejecución del proyecto incluye las siguientes etapas:

- Preparación y preparación: un mes
- Duración de la auditoría: dos meses
- Análisis de resultados e informe: 1 mes

Costos:

El examen que se llevará a cabo tiene como objetivo cumplir con los requisitos para obtener el título en Tecnologías de la Información de la Universidad Nacional de Chimborazo, por lo que no se generará ningún valor económico.

Recursos Necesarios:

Los siguientes recursos son necesarios para completar el proyecto:

- Equipo de auditoría informática
- Acceso a la infraestructura de red
- Herramientas de evaluación de seguridad
- Personal interno que colabore con el proyecto

Riesgos y Mitigaciones:

Se identifican riesgos potenciales que podrían afectar la ejecución del proyecto, como la falta de cooperación del personal interno o la detección de vulnerabilidades de red críticas. Se recomienda la comunicación efectiva con el personal y la implementación de soluciones correctivas inmediatas en caso de hallazgos críticos.

Conclusiones:

En términos de objetivos, cronograma, costos y recursos necesarios, el estudio de factibilidad indica que el proyecto es viable. La decisión de iniciar el proyecto de auditoría informática de seguridad física en el área de redes de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo se basa en el hecho de que los beneficios esperados superan los costos asociados.

FASE DE PLANIFICACIÓN

Objetivo: establecer el rumbo del proyecto mediante la creación de un plan detallado. Esto incluye definir el alcance, establecer objetivos específicos, desarrollar el cronograma, estimar los costos y planificar la gestión de riesgos. El resultado es un plan de gestión del proyecto que guiará las actividades y recursos necesarios para alcanzar los objetivos del proyecto de manera organizada y eficiente.

En la siguiente tabla 6, se presenta el plan del proyecto de Auditoría de seguridad física en el área de redes, alineada con la norma ISO/IEC 27001 y se adjunta enlace de calendario: Calendario1.pdf

Tabla 6. Planificación

Actividad	Descripción	Responsable	Fecha Inicio	Fecha Fin
Revisión de Políticas de Seguridad	Analizar las políticas actuales frente a la norma ISO 27001.	Director de Cómputo	Mayo 2024	Mayo 2024
Evaluación de Documentación de Equipos	Revisar los manuales y registros de mantenimiento de equipos.	Técnico de Laboratorios	Junio 2024	Julio 2024
Análisis de la Infraestructura	Realizar un inventario y estado de la infraestructura tecnológica.	Técnico de Laboratorios	Julio 2024	Agosto 2024

La tabla describe las actividades clave de la fase de planificación de un proyecto de auditoría de seguridad física en el área de redes, alineado con la norma ISO/IEC 27001.

FASE DE EJECUCIÓN

Objetivo: es la implementación del plan del proyecto a través de la coordinación de personas y recursos y la implementación de las actividades planificadas. En esta fase se realiza el trabajo necesario para cumplir con los requisitos del proyecto, se gestionan las expectativas de las partes interesadas y se asegura la calidad del trabajo. El objetivo es producir los resultados del proyecto según lo planeado.

Preparación

Revisión de la documentación: revisión la documentación del proyecto, incluido el plan del proyecto, la matriz de responsabilidades y los procedimientos de revisión.

Asignación de tareas: asignación de tareas al miembro auditor según su rol y responsabilidad.

En la siguiente tabla 7, se realiza la asignación de cada tarea y su responsable, para correcta ejecución de la auditoría.

Tabla 7. Asignación de tareas

Actividad	Responsable	Tarea	Fecha de Inicio	Fecha de Finalización	Comentarios
Revisión de Políticas de Seguridad	Autor	Analizar las políticas actuales frente a la norma ISO 27001.	28/05/2024	30/05/2024	Asegurar el cumplimiento de normativas.
Evaluación de Documentación de Equipos	Autor	Revisión del estado de los equipos de red. Evaluación del etiquetado y organización del cableado.	01/06/2024	12/06/2024	Asegurar cumplimiento con ISO 27001.
Análisis de la Infraestructura	Autor	Realizar un inventario y estado de la infraestructura tecnológica.	13/06/2024	20/06/2024	Asegurar la correcta implementación.

La tabla 7 detalla las actividades específicas, responsables, fechas y comentarios para el proyecto de auditoría de seguridad física en el área de redes.

1. **Revisión de Políticas de Seguridad**

   - Anexo de políticas de seguridad:
   Políticas de Seguridad de la Información UNACHv2.pdf

2. **Evaluación de Documentación de Equipos**
   - Anexo Manual de Descripción, Valoración y Clasificación de Puestos: https://www.unach.edu.ec/images/reglamentos/Manuales/2022/MANUAL%20DE%20DVC%20DE%20PUESTOS%20UNACH%20CODIFICADO%20A%20DICIEMBRE2021-signed.pdf
   - Anexo Firewall:

FIREWALL.png

- Anexo Sistema de Gestión de la Red:
  Juniper mist.png
- Anexo Reporte Semanal de Alertas:
  Reporte semanal UNACH-2024-06-16-0238-0500_36825.pdf
- Anexo Infraestructura de Red:
  UNACH-PGA-04-02-INFRAESTRUCTURA DE REDES.docx

3. Inventario de equipos de red del BLOQUE A de la facultad de energía.

PISO 3

En la siguiente tabla 8, se presenta el inventario de los switches del piso 3:

Tabla 8. Switches piso 3

Switch						
N°	**Piso**	**Ubicación**	**Marca**	**Modelo**	**N° de puertos**	**Características**
1	3	LabA308	CISCO	CATALYST 3750X	24 UTP	
2	3	LabA308	CISCO	CATALYST 2960 PLUS	24 UTP	
3	3	LabA308	JUNITER	SKU	47 UTP	
4	3	LabA308	JUNITER	EX4100	24 UTP	
5	3	LabA308	HP	PROCUBER 4000M	64 UTP	
6	3	LabA300	CISCO	CATALYST 2960	24 UTP	
7	3	LabA303	CISCO	CATALYST 2961	25 UTP	
8	3	LabA304	CISCO	CATALYST 2962	26 UTP	
9	3	LabA307	CISCO	CATALYST 2963	27 UTP	
10	3	LabA310	CISCO	CATALYST 2964	28 UTP	
11	3	LabA311	CISCO	CATALYST 2965	29 UTP	

La tabla 8 describe que en LabA308 hay cinco switches: CISCO CATALYST 3750X (24 puertos), CISCO CATALYST 2960 PLUS (24 puertos), JUNITER SKU (47 puertos), JUNITER EX4100 (24 puertos) y HP PROCUBER 4000M (64 puertos). En LabA300 está el CISCO CATALYST 2960 (24 puertos), en LabA303 el CISCO CATALYST 2961 (25 puertos), en LabA304 el CISCO CATALYST 2962 (26 puertos), y en LabA307 el CISCO CATALYST 2963 (27 puertos).

En la siguiente tabla 9, se presenta el inventario de los racks del piso 3:

Tabla 9. Racks piso 3

Racks			
N°	**Piso**	**Ubicación**	**Marca**
1	3	A308	THALER
2	3	A300	THALER
3	3	A303	THALER
4	3	A304	THALER
5	3	A307	THALER
6	3	A310	THALER
7	3	A311	THALER

La tabla 9 muestra que en el piso 3 hay 7 racks ubicados en distintas áreas, todos de la marca THALER. Los racks están distribuidos en las ubicaciones A308, A300, A303, A304, A307, A310 y A311.

En la siguiente tabla 10, se presenta el inventario de los Access point del piso 3:

Tabla 10. Access Point piso 3

Access Point			
N°	**Piso**	**Marca**	**Modelo**
1	3	Juniper	Mist ai
2	3	Juniper	Mist ai
3	3	Juniper	Mist ai
4	3	Juniper	Mist ai

La tabla 10 nos da a conocer que en el piso 3 hay 4 access points, todos de la marca Juniper y del modelo Mist AI.

En la siguiente tabla 11, se presenta el inventario de los patch panles del piso 3:

Tabla 11. Patch Panel piso 3

Patch Panel				
N°	**Piso**	**Ubicación**	**Marca**	**N° de Puertos**
1	3	A308	LEVITON	24
2	3	A308	LEVITON	24
3	3	A308	LEVITON	24
4	3	A308	LEVITON	24
5	3	A300	LEVITON	24
6	3	A303	LEVITON	24
7	3	A304	LEVITON	24

8	3	A307	LEVITON	24
9	3	A309	LEVITON	24
10	3	A310	LEVITON	24
11	3	A311	LEVITON	24

La tabla 11 muestra que en el piso 3 hay 11 patch panels de la marca LEVITON, cada uno con 24 puertos, ubicados en las siguientes áreas: A308 (4 patch panels), A300, A303, A304, A307, A309, A310 y A311.

PISO 2

En la siguiente tabla 12, se presenta el inventario de los switches del piso 2:

Tabla 12. Switches piso 2

Switch						
N°	**Piso**	**Ubicación**	**Marca**	**Modelo**	**N° de puertos**	**Características**
1	2	PASILLO	CISCO	CATALYST 2960	24UTP	
2	2	PASILLO	CISCO	CATALYST 2960	24UTP	
3	2	PASILLO	JUNITER	EX4100	24UTP	
4	2	CONSULTORIOS TECNOLOGICOS	CISCO	CATALYS2960	24UTP	
5	2	CONSULTORIOS TECNOLOGICOS	3com	4226T	24UTP	

La tabla 12 describe que en el piso 2 hay 5 switches distribuidos en dos ubicaciones: Pasillo y Consultorios Tecnológicos. En el Pasillo, hay dos switches CISCO CATALYST 2960 y uno JUNITER EX4100, todos con 24 puertos UTP. En los Consultorios Tecnológicos, hay un switch CISCO CATALYST 2960 y otro 3com 4226T, también con 24 puertos UTP.

En la siguiente tabla 13, se presenta el inventario de los racks del piso 2:

Tabla 13. Racks piso 2

Racks			
N°	**Piso**	**Ubicación**	**Marca**
1	2	PASILLO	THALER
2	2	CONSULTORIOS TECNOLOGICOS	THALER

La tabla 13 muestra que en el piso 2 hay 2 racks: uno en el Pasillo y otro en Consultorios Tecnológicos, ambos de la marca THALER.

En la siguiente tabla 14, se presenta el inventario de los Access point del piso 2:

Tabla 14. Access Point piso 2

Access Point			
N°	**Piso**	**Marca**	**Modelo**
1	2	Juniper	Mist ai
2	2	Juniper	Mist ai
3	2	Juniper	Mist ai
4	2	Juniper	Mist ai

La tabla 14 nos da a conocer que en el piso 2 hay 4 access points, todos de la marca Juniper y del modelo Mist AI.

En la siguiente tabla 15, se presenta el inventario de los patch panles del piso 2:

Tabla 15. Patch Panel piso 2

Patch Panel				
N°	**Piso**	**Ubicación**	**Marca**	**N° de Puertos**
1	3	PASILLO	LEVITON	24
2	3	PASILLO	LEVITON	24
3	3	CONSULTORIO TECNOLOGICO	LEVITON	24

La tabla 15 describe que en el piso 3 hay 3 patch panels de la marca LEVITON, cada uno con 24 puertos. Dos están ubicados en el Pasillo y uno en el Consultorio Tecnológico.

PISO 1

En la siguiente tabla 16, se presenta el inventario de los switches del piso 1:

Tabla 16. Switches piso 1

Switch						
N°	**Piso**	**Ubicación**	**Marca**	**Modelo**	**N° de puertos**	**Características**
1	1	PASILLO	CISCO	CATALYS2960	24UTP	
2	1	PASILLO	JUNITER	EX4100	24UTP	

La tabla 16 muestra que en el piso 1 hay 2 switches: uno CISCO CATALYST 2960 con 24 puertos UTP y otro JUNITER EX4100 con 24 puertos UTP, ambos ubicados en el Pasillo.

En la siguiente tabla 17, se presenta el inventario de los racks del piso 1:

Tabla 17. Racks piso 1

Racks			
N°	**Piso**	**Ubicación**	**Marca**
1	1	PASILLO	THALER

La tabla 17 da a conocer que en el piso 1 hay 1 rack, ubicado en el Pasillo, de la marca THALER.

En la siguiente tabla 18, se presenta el inventario de los Access point del piso 1:

Tabla 18. Access Point piso 1

Access Point			
N°	**Piso**	**Marca**	**Modelo**
1	1	Juniper	Mist ai
2	1	Juniper	Mist ai
3	1	Juniper	Mist ai
4	1	Juniper	Mist ai

La tabla 18 muestra que en el piso 1 hay 4 access points, todos de la marca Juniper y del modelo Mist AI.

En la siguiente tabla 19, se presenta el inventario de los switches del piso 3:

Tabla 19. Patch Panels piso 1

Patch Panel				
N°	**Piso**	**Ubicación**	**Marca**	**N° de Puertos**
1	1	PASILLO	LEVITON	24

La tabla 19 describe que en el piso 1 hay 1 patch panel de la marca LEVITON con 24 puertos, ubicado en el Pasillo.

4. EVALUACIÓN HARDWARE DE RED

En la siguiente tabla 20, se presenta la evaluación de los switches de todos los pisos del BLOQUE A:

Tabla 20. Evaluación de los switches del BLOQUE A según Anexo 4:

SWITCH	
Instalación Física	100%
Protección contra Daños Físicos	97,22%
Seguridad física	96,30%
Mantenimiento y Revisión	0,00%
Cumplimiento de Normativas	85,50%
TOTAL	**75.20%**

Observación: Los resultados obtenidos de la evaluación del switch en cuanto a su instalación física, protección contra daños, seguridad, mantenimiento, y cumplimiento de normativas muestran un panorama variado. Se destaca un alto grado de cumplimiento en aspectos como la instalación física y la protección contra daños físicos, lo que indica una implementación adecuada de medidas de seguridad física. Sin embargo, se identifican áreas de mejora significativas, especialmente en el mantenimiento y la revisión periódica del switch, donde se evidencia una falta de registros y seguimiento. Esto resalta la necesidad de establecer procedimientos más rigurosos para garantizar su funcionamiento óptimo a lo largo del tiempo.

En la siguiente tabla 21, se presenta la evaluación del cableado estructurado:

Tabla 21. Evaluación del cableado de red del BLOQUE A según Anexo 4:

CABLEADO	
Instalación Física	44,44%
Protección contra Daños Físicos	97,22%
Seguridad	96,30%
Mantenimiento y Revisión	0,00%
Cumplimiento de Normativas	0,00%
TOTAL	**47.99%**

Observación: Los resultados de la evaluación del cableado muestran un nivel variable de cumplimiento. Se observa un alto grado de protección contra daños físicos y seguridad del cableado, lo que indica una buena implementación de medidas de seguridad física. Sin embargo, existen deficiencias significativas en la instalación física del cableado (falta de organización y etiquetado), el mantenimiento (no existen mantenimientos, ni revisiones periódicas) y el cumplimiento de normativas, con puntajes bajos en estos aspectos. Es crucial implementar acciones correctivas para mejorar la instalación y el mantenimiento del cableado, así como asegurar el cumplimiento de las normativas establecidas para garantizar la integridad y seguridad de la red.

En la siguiente tabla 22, se presenta la evaluación de los racks:

Tabla 22. Evaluación de los racks del BLOQUE A según Anexo 4:

RACKS	
Instalación Física	100%
Protección contra Daños Físicos	95%
Seguridad física	90%
Mantenimiento y Revisión	0,00%
Cumplimiento de Normativas	85,50%
TOTAL	**74.30%**

Observación: Los resultados de la evaluación de los racks muestran un alto nivel de cumplimiento en la instalación física y la protección contra daños físicos, lo que indica una implementación adecuada de medidas de seguridad. Sin embargo, se identifican deficiencias en el mantenimiento y la revisión, donde no se evidencian registros ni seguimiento.

En la siguiente tabla 23, se presenta la evaluación de los Access point:

Tabla 23. Evaluación de los access point del BLOQUE A según Anexo 4:

ACCESS POINT	
Instalación Física del	100%
Protección contra Daños Físicos	100%
Seguridad de los	100%
Mantenimiento y Revisión	0,00%
Cumplimiento de Normativas	97,33%
TOTAL	**79.67%**

Observación: Los resultados de la evaluación de los Access Points (AP) muestran un alto nivel de cumplimiento en la instalación física, protección contra daños físicos y seguridad de los AP, lo que indica una implementación adecuada de medidas de seguridad. Sin embargo, se identifica una deficiencia en el mantenimiento y revisión, donde no se evidencian registros ni seguimiento. A pesar de esto, el cumplimiento de normativas es sólido, aunque existen áreas que pueden ser fortalecidas.

En la siguiente tabla 24, se presenta la evaluación de los patch panels:

Tabla 24. Evaluación de los patch panels del BLOQUE A según Anexo 4:

PATCH PANELS	
Instalación Física del	100%
Protección contra Daños Físicos	100%
Seguridad de los	100%
Mantenimiento y Revisión	0,00%
Cumplimiento de Normativas	95,69%
TOTAL	**79.54%**

Observación: Los resultados de la evaluación de los Patch Panels reflejan un alto nivel de cumplimiento en la instalación física, protección contra daños físicos y seguridad, lo que indica una implementación adecuada de medidas de seguridad. Sin embargo, se identifica una carencia en el mantenimiento y revisión, donde no se encuentran registros ni seguimiento. A pesar de ello, el cumplimiento de normativas es sólido, aunque se pueden fortalecer ciertos aspectos.

PERSONAL

En la siguiente tabla 25, se presenta la evaluación del personal técnico del Centro de Unidades Educativas de la UNACH:

Tabla 25. Evaluación al personal

Cargo	Capacitación		Experiencia		Formación		Punt.
Director Del Centro De Cómputo	1 curso = 1 2 cursos = 2 3 cursos = 3 4 cursos = 4 ≥5 cursos = 5	4	0 - 1 años = 1 2 – 3 años = 2 4 – 5 años = 3 6 – 7 años = 4 ≥8 años = 5	5	Nivel Técnico = 1 Tercer Nivel = 2 Especialización = 3 Maestría = 4 Doctorado = 5	4	13/15
Analista de TI	1 curso = 1 2 cursos = 2 3 cursos = 3 4 cursos = 4 ≥5 cursos = 5	5	0 - 1 años = 1 2 – 3 años = 2 4 – 5 años = 3 6 – 7 años = 4 ≥8 años = 5	5	Nivel Técnico = 1 Tercer Nivel = 2 Especialización = 3 Maestría = 4 Doctorado = 5	3	13/15
							25/30

En la siguiente tabla 26, se presenta el puntaje de la evaluación del personal:

Tabla 26. Puntaje

Personal	Puntaje	Estado
Total	25/30	83.33%

La observación sobre los datos presentados indica que el personal, tiene un nivel significativo de capacitación y experiencia en sus respectivos roles. Cuentan con una calificación alta en formación, indicando un nivel avanzado de educación en sus áreas de especialización.

ENTORNO

En la siguiente tabla 27, se presenta la evaluación del entorno del BLOQUE A de la facultad de ingeniería de la UNACH:

Tabla 27. Evaluación del entorno del BLOQUE A según Anexo 4:

ENTORNO	
Seguridad Física	75,71%
Seguridad Ambiental	25,00%
Cumplimiento de Normativas	71%
TOTAL	**57.24%**

La evaluación del entorno en la Universidad Nacional de Chimborazo (UNACH) reveló que la seguridad física del entorno obtuvo un 75,71%, el cumplimiento de normativas un 71%, y la seguridad ambiental un preocupante 25%, resultando en un total de 57,24%. Estos resultados indican que, aunque la seguridad física y el cumplimiento normativo son relativamente aceptables, la baja calificación en seguridad ambiental requiere atención urgente.

FASE DE MONITOREO

Revisión de la Documentación Existente sobre Políticas y Procedimientos

- **Meta:** Revisar toda la documentación relacionada con las políticas y procedimientos de seguridad.
- **Resultados:** Identificar las áreas que necesitan actualización para cumplir con ISO 27001.

Evaluación de la Infraestructura de Red y Sistemas Informáticos

- **Meta:** Evaluar al menos el 90% de la infraestructura de red y sistemas informáticos.
- **Resultados:** Crear un inventario detallado y documentar el estado actual de la infraestructura.

Entrevistas con el Personal Clave

- **Meta:** Realizar entrevistas con todos los miembros del personal clave.
- **Resultados:** Obtener información detallada sobre las prácticas y procedimientos de seguridad.

Verificación del Cumplimiento de Normativas

- **Meta:** Verificar el 100% del cumplimiento con las normativas ISO 27001.
- **Resultados:** Documentar las áreas de cumplimiento y aquellas que necesitan mejoras.

Elaboración de Informe y Recomendaciones

- **Meta:** Elaborar un informe final que incluya todas las recomendaciones pertinentes.
- **Resultados:** Crear un informe detallado que resuma los hallazgos y proporcione recomendaciones específicas.

DEFINICIÓN Y CÁCULO DE LOS INDICADORES

Una vez definido el plan de contingencia para la gestión de seguridad física en el área de redes de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo, se

establecieron los **índices de evaluación y seguimiento** para medir la efectividad de las acciones correctivas propuestas. A continuación, se explica detalladamente cómo se obtuvieron estos índices basados en el análisis del informe de auditoría, los hallazgos específicos y los requerimientos de la norma ISO 27001:

1. Índice de Cumplimiento de Normativas

- **Análisis Inicial**: El informe de auditoría indicó un nivel de cumplimiento normativo del 71% en relación con los estándares de la norma ISO 27001. Se identificaron deficiencias en la implementación de políticas de seguridad, falta de revisiones periódicas y ausencia de documentación actualizada. Estas deficiencias fueron clasificadas como un riesgo de gravedad y probabilidad altas, ya que el incumplimiento de normativas podría conllevar sanciones y comprometer la seguridad de la información.
- **Definición del Índice**: A partir de esta situación, se estableció como meta alcanzar un ≥ 90% de cumplimiento anual en el próximo año. Esta cifra se determinó considerando que el cumplimiento de la norma ISO 27001 exige una revisión periódica de políticas y auditorías internas trimestrales. Se programaron 4 auditorías trimestrales, una en cada trimestre del año, para evaluar y ajustar el cumplimiento.
- **Cálculo del Índice**: Cada auditoría trimestral incluirá la revisión de políticas, procedimientos y controles establecidos en la norma, y se asignará un puntaje de conformidad basado en los hallazgos. El índice se obtendrá sumando los resultados de las 4 auditorías, con el objetivo de ver una mejora progresiva en cada evaluación. La meta de ≥ 90% se estableció para asegurar que las políticas y procedimientos se mantengan alineados con los requisitos de la norma.

2. Índice de Incidentes

- **Análisis Inicial**: El informe de auditoría registró un índice de incidentes del 47.99% en la infraestructura de red debido a problemas como la falta de organización del cableado y el mantenimiento deficiente de equipos críticos (switches, racks y access points). Este índice se calculó dividiendo el número de incidentes registrados entre el número total de equipos evaluados, reflejando una situación preocupante en términos de continuidad operativa y disponibilidad de servicios.
- **Definición del Índice**: Se estableció como meta reducir el índice de incidentes a ≤ 15% anuales. Este objetivo se fijó considerando que la reorganización del cableado y la implementación de un programa de mantenimiento trimestral deberían reducir significativamente la frecuencia de fallos y problemas operativos.
- **Cálculo del Índice**: El índice de incidentes se evaluará trimestralmente, registrando el número de incidentes que ocurra en cada trimestre y comparándolo con el estado inicial. Para calcularlo, se dividirá el número de incidentes en el trimestre por el número total de equipos evaluados y se multiplicará por 100 para obtener el porcentaje de incidentes. La meta es ver una reducción continua, con una disminución progresiva hasta alcanzar el objetivo de ≤ 15% anual.

3. Tiempo de Respuesta Ante Incidentes Físicos

- **Análisis Inicial**: El informe reflejó tiempos de respuesta inadecuados ante incidentes físicos, con un promedio de 1 hora y 20 minutos. Esto se atribuyó a la falta de procedimientos claros y responsables asignados para cada tipo de incidente. Se consideró que la lentitud en la respuesta aumentaba la gravedad de los incidentes y el tiempo de recuperación.
- **Definición del Índice**: Se estableció como meta reducir el tiempo de respuesta a ≤ 30 minutos, garantizando una intervención rápida y eficiente en incidentes críticos (como fallos de equipos o problemas ambientales). Esta cifra se determinó considerando la capacidad de respuesta esperada según la norma ISO 27001 y las prácticas recomendadas en la gestión de incidentes.
- **Cálculo del Índice**: El tiempo de respuesta se medirá en cada incidente registrado. Se documentará el tiempo transcurrido desde que se detecta el incidente hasta que se inicia la acción correctiva. La media de estos tiempos se calculará trimestralmente, con el objetivo de ver una mejora progresiva hasta alcanzar y mantener el tiempo de respuesta ≤ 30 minutos.

FASE DE CIERRE

Objetivo: formalizar la aceptación del proyecto o una de sus fases, y realizar todas las actividades necesarias para concluirlo de manera organizada y controlada. Esto incluye completar todas las tareas del proyecto, entregar formalmente el proyecto al cliente o patrocinador, recopilar y documentar las lecciones aprendidas, liberar y reasignar recursos, cerrar contratos con proveedores y socios, y actualizar y archivar todos los documentos y registros del proyecto. En esencia, la fase de cierre garantiza que el proyecto se finaliza de manera controlada y documentada, y que todos los aspectos administrativos y contractuales se resuelven adecuadamente.

Carta de presentación:

Mag.

Javier Haro

DIRECTOR DEL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

De mi consideración:

Espero que este mensaje le encuentre bien. Me es grato informarle que hemos concluido el proceso de "Auditoría Informática de la Seguridad Física en el Área de Redes del Edificio A en la Facultad de Ingeniería de la Universidad Nacional de Chimborazo, de acuerdo con la norma ISO 27001".

Asimismo, le invito a la sesión de presentación del informe final, la cual se realizará el 29 de julio de 2024, en el aula 311 de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo.

Saludos cordiales,

Srta. Ivana Tenorio
C.I. 0803589068
AUDITOR

Informe final de auditoría informática:

Mag.

Javier Haro

DIRECTOR DEL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

De mi consideración:

Tras haber completado la Auditoría Informática de la Seguridad Física en el Área de Redes del Edificio A en la Facultad de Ingeniería de la Universidad Nacional de Chimborazo, utilizando la norma ISO 27001, me corresponde emitir una opinión sobre el cumplimiento de esta norma.

Los aspectos revisados para asegurar el cumplimiento incluyen: gestión de activos, control de acceso, seguridad física y ambiental, operaciones de seguridad, comunicaciones de seguridad, adquisición, desarrollo y mantenimiento de sistemas de información, relaciones con proveedores, gestión de incidentes de seguridad de la información, aspectos de seguridad de la información en la gestión de la continuidad del negocio, y cumplimiento de requisitos legales.

En mi opinión, el área de redes del Edificio A de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo cumple satisfactoriamente con la mayoría de los componentes evaluados. No obstante, se han identificado algunas áreas que requieren mejoras para cumplir completamente con las obligaciones y mantener un nivel óptimo de seguridad.

Atentamente,

Sñrta. Ivana Tenorio
C.I. 0803589068
AUDITOR

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

4.1. Resultados

A partir del informe de auditoría de la seguridad física en el área de redes del Bloque A de la Facultad de Ingeniería, se obtuvieron los siguientes resultados:

El Número de Cumplimiento de Normativas es: 71%, identificado como el nivel actual de cumplimiento normativo en relación con los estándares ISO 27001. Este valor refleja deficiencias en la actualización de políticas y auditorías internas.

El Número de Índice de Incidentes es: 47.99%, debido a problemas de mantenimiento y organización del cableado, lo que impacta negativamente en la infraestructura crítica de red.

El Tiempo de Respuesta Ante Incidentes Físicos es: 1 hora y 20 minutos en promedio, evidenciando una respuesta lenta ante problemas físicos, como fallos de equipos o eventos ambientales.

Adjunto matriz validación del plan de contingencia a través del anexo 5.

Plan de Contingencia Detallado para la Infraestructura de Red

1. Identificación de Riesgos

Basado en el informe de auditoría, se han identificado los siguientes riesgos:

- **Riesgo de Incumplimiento Normativo:** Falta de auditorías periódicas y documentación actualizada (71%), detallado en las tablas 20, 21, 22, 23 y 24.
- **Riesgo de Fallas en Equipos Críticos:** Cableado desorganizado y sin mantenimiento. Falta de medidas de protección física, detallado en las tablas 20, 21, 22, 23 y 24.
- **Riesgo de Seguridad Ambiental Deficiente:** Sin sistemas de detección de incendios ni respaldo de energía (25%), detallado en la tabla 24.

2. Evaluación de Riesgos

Se ha evaluado cada riesgo considerando la gravedad y probabilidad de ocurrencia:

- **Gravedad y Probabilidad Alta:**
  - Incumplimiento normativo y fallos en infraestructura crítica, detallado en la tabla 21.
- **Gravedad Alta y Probabilidad Media:**
  - Falta de medidas de seguridad ambiental, detallado en la tabla 24.

3. Establecimiento de Prioridades y Medidas Correctivas

1. **Normativas:**
   - Medida: Auditorías trimestrales ISO 27001.
   - Indicador: Aumentar cumplimiento a ≥ 90%.
2. **Infraestructura Crítica:**
   - Medida: Reorganización del cableado y mantenimiento de equipos.
   - Indicador: Índice de Incidentes ≤ 15% anuales.
3. **Seguridad Ambiental:**
   - Medida: Instalar sistemas de detección de incendios y respaldo de energía.
   - Indicador: Reducir riesgos de incidentes ambientales a ≤ 10% de impacto.

4. Procedimiento de Implementación

Normativas

- **Acción:** Actualizar políticas internas según ISO 27001 y programar auditorías internas cada 3 meses.
- **Responsable:** Director de Cómputo.
- **Cronograma:**
  - **Auditoría 1:** Octubre 2024
  - **Auditoría 2:** Enero 2025
  - **Auditoría 3:** Abril 2025

Infraestructura Crítica

- **Acción:** Organización del cableado, instalación de etiquetas, y revisión de switches.
- **Responsable: T**écnico de Laboratorios.
- **Cronograma:**
  - Organización y etiquetado: Octubre 2024
  - Revisión de switches: Noviembre 2024

Seguridad Ambiental

- **Acción:** Instalación de sensores de humo y respaldo energético en el área de servidores.
- **Responsable:** Director de Cómputo y Proveedores.
- **Cronograma:**
  - Instalación de sistemas: Noviembre 2024
  - Pruebas de funcionamiento: Diciembre 2024

1. Asignación de Responsabilidades y Gráfico RACI

En la tabla 28 se muestran las tareas a realizar en el plan:

Tabla 28. Tareas y responsabilidades

Tarea	Responsable (R)	Aprobador (A)	Consultado (C)	Informado (I)
Auditoría Normativa	Director de Cómputo	Decano	Personal Técnico	Directores
Organización de Cableado	Técnico de Labor.	Director de Cómputo	Proveedores	Personal Técnico
Seguridad Ambiental	Director de Cómputo	Decano	Proveedores	Personal Afectado

2. Gráfico de Evaluación de Riesgos

En la gráfica 2, se representan los riesgos encontrados en el informe de auditoría.

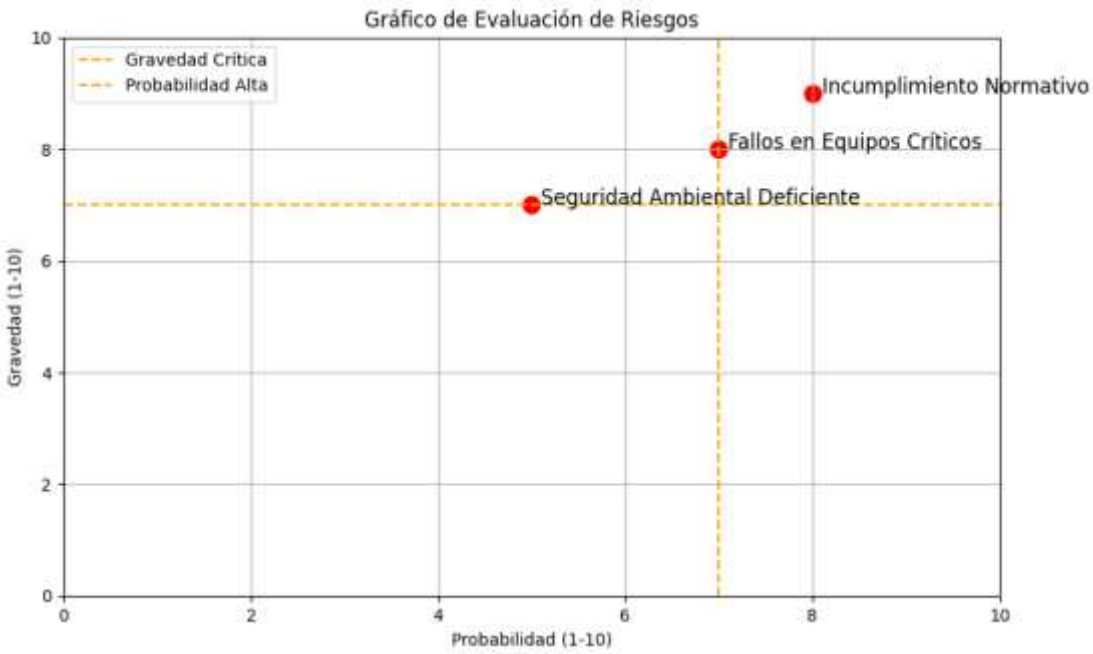


Ilustración 2. Riesgos

Descripción:

El gráfico de evaluación de riesgos, donde se representan la probabilidad y gravedad de los principales riesgos identificados:

- **Incumplimiento Normativo**: Alta gravedad y probabilidad.
- **Fallos en Equipos Críticos**: Alta gravedad y probabilidad media.
- **Seguridad Ambiental Deficiente**: Gravedad media y probabilidad baja.

El gráfico muestra cómo estos riesgos se ubican en función de su impacto y la probabilidad de ocurrencia, facilitando su priorización y manejo.

7. Monitoreo y Revisión del Plan

- **Frecuencia:** Mensual.
- **Responsable:** Equipo de Auditoría Interna.
- **Revisión de Normas:** Trimestral.
- **Evaluación de Resultados:** Reportes mensuales de progreso y cumplimiento normativo.

8. Índices de Evaluación y Seguimiento

Número de Cumplimiento de Normativas

Meta: Alcanzar y mantener un nivel de cumplimiento anual de ≥ 90%.

Descripción: El índice de cumplimiento de normativas mide el grado de conformidad con los requisitos de la norma ISO 27001. Se evalúa el cumplimiento de políticas, procedimientos y controles de seguridad implementados para asegurar que la organización opere de acuerdo con los estándares establecidos.

Cómo se Obtiene:

Se realizarán 4 auditorías internas anuales (trimestrales), donde se revisarán todos los procesos y procedimientos alineados con la norma ISO 27001.

Cada auditoría incluirá la revisión de documentos, entrevistas con el personal y la verificación de controles implementados en el área de redes.

Al finalizar cada auditoría, se emitirá un reporte detallado con el porcentaje de cumplimiento alcanzado, identificando las áreas conformes y no conformes.

Indicador: El indicador de este índice será el porcentaje total de conformidad alcanzado en cada auditoría trimestral. Este porcentaje se calcula sumando el cumplimiento de cada control revisado en la auditoría y dividiéndolo entre el total de controles exigidos.

Fórmula:

$$Cumpimiento\ de\ normativas = \frac{Controles\ Conformes}{\text{Total de Controles Evaluados}} * 100$$

Evidencia: Reportes trimestrales con resultados detallados de las auditorías y acciones correctivas propuestas para mejorar el cumplimiento.

Número de Índice de Incidentes

Meta: Reducir a ≤ 15% el número de incidentes anuales relacionados con la infraestructura crítica.

Descripción: Este índice mide la cantidad de incidentes que afectan la infraestructura física y tecnológica en el área de redes, tales como fallos en equipos (switches, racks) y problemas en la organización del cableado. La meta es reducir la frecuencia de estos incidentes mediante mantenimiento preventivo y correctivo.

Cómo se Obtiene:

El índice se calculará trimestralmente, registrando el número de incidentes ocurridos en cada trimestre.

Se comparará el número de incidentes con el número total de equipos críticos evaluados, como switches, access points, y racks.

Se implementarán reportes trimestrales de fallos, analizando las causas y el impacto de cada incidente, así como el tiempo de recuperación.

Indicador: Porcentaje de incidentes en relación con el total de equipos críticos.

Fórmula:

$$\text{Índices de Incidentes} = \frac{\text{Número de Incidentes}}{\text{Total de Equipos Evaluados}} * 100$$

Evidencia: Reportes trimestrales con el número de incidentes y su impacto, así como acciones correctivas aplicadas para reducir su ocurrencia.

Tiempo de Respuesta Ante Incidentes Físicos

Meta: ≤ 30 minutos de tiempo de respuesta ante incidentes físicos.

Descripción: Este índice mide la rapidez con la que se responde a incidentes físicos en la infraestructura tecnológica (e.g., fallos de equipos, problemas ambientales). Su objetivo es minimizar el tiempo de inactividad y asegurar una intervención oportuna ante situaciones críticas.

Cómo se Obtiene:

Se registrará el tiempo de respuesta desde la detección de un incidente físico hasta la ejecución de la primera acción correctiva.

Se monitoreará cada incidente mediante un sistema de registro de tiempos de respuesta y se calculará el promedio de respuesta en cada trimestre.

La implementación de protocolos claros y la asignación de responsables asegurarán una respuesta rápida y eficiente.

Indicador: Tiempo promedio de respuesta ante incidentes físicos, medido en minutos.

Fórmula:

$$Tiempo\ de\ Respuestas = \frac{Suma\ de\ Tiempo\ de\ Respuestas}{\text{Número Total de Incidentes}}$$

Evidencia: Registro detallado de incidentes, tiempos de respuesta y acciones tomadas.

A continuación, en la tabla 29, tenemos el Cronograma General de Implementación del Plan de Contingencia:

Tabla 29. Cronograma

Fase	Actividad	Responsable	Fecha Inicio	Fecha Fin	Indicador de Éxito
Fase 1: Evaluación	Auditoría Normativa	Director de Cómputo	Octubre 2024	Abril 2025	Cumplimiento ≥ 90%
Fase 2: Mantenimiento	Organización y Mantenimiento de Equipos	Técnico de Laboratorios	Octubre 2024	Diciembre 2024	Incidentes ≤ 15% trimestral
Fase 3: Seguridad Ambiental	Instalación de Sistemas de Detección y Respaldo	Director de Cómputo	Noviembre 2024	Febrero 2025	Sistemas instalados y operativos
Fase 4: Supervisión y Control	Evaluaciones Trimestrales de Vulnerabilidades	Director de Cómputo	Octubre 2024	Septiembre 2025	4 evaluaciones anuales completadas

Nota: Este plan se revisará trimestralmente para asegurar su efectividad y actualización continua.

4.2. Discusión

El análisis del Plan de Contingencia Detallado para la Infraestructura de Red muestra un enfoque estructurado para mitigar los riesgos críticos identificados durante la auditoría. Los riesgos se clasifican en tres categorías principales: incumplimiento normativo, fallas en equipos críticos y seguridad ambiental deficiente. El incumplimiento normativo, que alcanza un 71%, representa el mayor riesgo debido a la falta de auditorías periódicas y documentación actualizada, lo cual afecta la conformidad con la norma ISO 27001. A este riesgo se suman las fallas en equipos críticos, relacionadas con cableado desorganizado y la falta de mantenimiento, que presentan una gravedad alta y probabilidad media. Finalmente, el riesgo de seguridad ambiental deficiente, caracterizado por la falta de sistemas de detección de incendios y respaldo de energía, posee una gravedad media y probabilidad baja.

Para cada riesgo, se han establecido medidas correctivas basadas en la evaluación de su gravedad y probabilidad de ocurrencia. En el caso del incumplimiento normativo, se propone la realización de auditorías trimestrales con el objetivo de incrementar el nivel de cumplimiento a $\geq 90\%$. Esta medida, acompañada de la actualización de políticas internas y la asignación de responsabilidades al Director de Cómputo, busca asegurar la conformidad continua con la normativa vigente. En cuanto a las fallas en equipos críticos, se han definido acciones para la reorganización del cableado y el mantenimiento de equipos con el fin de reducir los incidentes a $\leq 15\%$ anuales. Para abordar la seguridad ambiental, se recomienda la instalación de sensores de humo y respaldos de energía que disminuyan el impacto de posibles incidentes a $\leq 10\%$.

El cronograma de implementación del plan se extiende desde octubre de 2024 hasta septiembre de 2025 y se divide en fases que abordan cada grupo de riesgos de manera sistemática. La primera fase se centra en las auditorías normativas, mientras que la segunda y tercera fases incluyen la organización y mantenimiento de la infraestructura crítica y la mejora de la seguridad ambiental. A lo largo de estas fases, se han asignado responsabilidades específicas a diferentes actores, como el Director de Cómputo y los Técnicos de Laboratorio, y se han definido indicadores claros para medir el éxito de cada acción implementada, como el índice de incidentes y el tiempo de respuesta ante contingencias.

El monitoreo y la revisión continua del plan se realizarán mensualmente, con evaluaciones trimestrales por parte del equipo de auditoría interna. Se elaborarán reportes detallados del progreso y del cumplimiento normativo, con el fin de identificar áreas de mejora y garantizar la efectividad del plan. Adicionalmente, se ha incluido un gráfico de evaluación de riesgos que visualiza la gravedad y la probabilidad de cada riesgo, facilitando la toma de decisiones y la asignación de recursos.

Se puede decir, que la implementación del Plan de Contingencia para la Infraestructura de Red refleja una metodología orientada a la mejora continua, con una estructura clara y medidas correctivas alineadas a las mejores prácticas internacionales. La definición de prioridades, un cronograma detallado y un sistema de monitoreo constante garantizan que la organización esté preparada para enfrentar contingencias de manera efectiva y alineada a las normativas internacionales, contribuyendo así a un entorno tecnológico seguro y resiliente.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

En la auditoría de seguridad física en el área de redes del bloque A de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo, se observó que la instalación de equipos es adecuada, pero el mantenimiento y la revisión son deficientes. La seguridad física del entorno es relativamente buena, aunque la seguridad ambiental es insatisfactoria. La red muestra un rendimiento aceptable en términos de latencia y velocidad de descarga, pero la velocidad de carga es deficiente. Las vulnerabilidades detectadas son en su mayoría de baja severidad. En general, se identificaron áreas críticas que necesitan ser mejoradas para optimizar la seguridad física y el rendimiento de la red.

Investigar la norma ISO 27001 enfocada en seguridad física de red reveló su importancia en la protección integral de la infraestructura de TI de una organización. La norma ISO 27001 establece un marco de gestión para asegurar la confidencialidad, integridad y disponibilidad de la información, incluyendo aspectos clave de seguridad física que son fundamentales para salvaguardar los activos críticos y la infraestructura de red. Al implementar los controles y requisitos especificados por la norma, las organizaciones pueden fortalecer su capacidad para prevenir y mitigar amenazas físicas, garantizar el cumplimiento normativo y mantener un entorno seguro para la operación de sus redes. La norma proporciona directrices claras para evaluar, implementar y mantener medidas de seguridad física, asegurando así una protección robusta y continua frente a riesgos y vulnerabilidades.

La auditoría realizada reflejó un desempeño satisfactorio en la instalación física de equipos como switches, racks y access points, con un cumplimiento del 100% en este aspecto; sin embargo, se identificaron deficiencias críticas en el mantenimiento y revisión de dichos dispositivos, alcanzando un 0% en ambas categorías, lo cual representa un riesgo significativo para la continuidad operativa. En cuanto a la seguridad física del entorno, se obtuvo un 75.71%, mostrando un nivel aceptable en términos de protección de acceso y seguridad perimetral, aunque con margen de mejora. La principal área de preocupación radica en la seguridad ambiental, que se evaluó en solo un 25%, evidenciando carencias en sistemas de detección de incendios y respaldo energético. Esto subraya la necesidad urgente de implementar acciones correctivas en mantenimiento y seguridad ambiental para mitigar riesgos potenciales y fortalecer la resiliencia de la infraestructura tecnológica.

El plan de contingencia establece objetivos claros para mejorar la seguridad y el cumplimiento normativo en el Bloque A de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo. Con auditorías trimestrales, se busca alcanzar un $\geq$ 90% de cumplimiento normativo. Además, se reducirá el índice de incidentes a $\leq$ 15% mediante mantenimiento regular y reorganización del cableado. Las 4 evaluaciones anuales de vulnerabilidad identificarán proactivamente riesgos, y un tiempo de respuesta $\leq$ 30 minutos garantizará una intervención eficiente ante incidentes físicos. Estos indicadores aseguran un monitoreo continuo, también permiten ajustes para mantener la seguridad y eficiencia en la gestión tecnológica.

5.2. Recomendaciones

Implementar un programa de mantenimiento regular y exhaustivo para los equipos de red, que incluya inspecciones periódicas y revisiones detalladas. Además, mejorar la seguridad ambiental mediante la instalación de sistemas de control climático adecuados y medidas de protección contra factores ambientales adversos. Para la velocidad de carga deficiente, considerar la optimización de la infraestructura de red y la actualización de los equipos si es necesario.

Adoptar e implementar los controles y directrices especificados en la norma ISO 27001 para fortalecer la seguridad física de la red. Esto incluye la realización de evaluaciones de riesgos, la implementación de medidas de seguridad adecuadas y la capacitación continua del personal en prácticas de seguridad. Asegúrate de realizar auditorías regulares para mantener el cumplimiento y ajustar las medidas según sea necesario.

Establecer un plan de acción para abordar las deficiencias en mantenimiento y revisión de equipos, priorizando la implementación de prácticas de mantenimiento regular. Mejorar la seguridad ambiental mediante la implementación de sistemas adecuados para controlar temperatura y humedad. Para la velocidad de carga deficiente, evaluar y optimizar la configuración de red, y considerar actualizaciones tecnológicas si es necesario. Reforzar la gestión de vulnerabilidades mediante la aplicación de parches y controles adicionales para reducir el porcentaje de vulnerabilidades de severidad media y alta.

Asegurar la efectividad del Plan de Contingencia mediante simulacros regulares y revisiones periódicas. Establecer mecanismos para evaluar y actualizar el plan con base en cambios en la infraestructura de red y lecciones aprendidas de incidentes anteriores. Garantizar que el personal esté adecuadamente capacitado en los procedimientos del plan y que se mantenga una comunicación fluida y efectiva durante la gestión de incidentes.

BIBLIOGRÁFIA

[1] J. Areitio, «Seguridad de la informacion. Redes, informática y sistemas de información,» Madrid, 2008.

[2] J. E. Mercado Rojas, «Modelo de gestión de seguridad de la información para el E-Gobierno,» Lima, 2016.

[3] B. A. Murillo Ávila, «Propuesta de Políticas de Seguridad de la Información para la Empresa Cárnicos La JOYA S.A.,» 2024.

[4] J. F. Rodriguez Rodriguez, «Proyecto de inversión para la creación de una empresa dedicada a consultoría de gestión de TI y seguridad de la información en la ciudad de Lima,» Lima, 2020.

[5] R. G. Potosi Bravo, «Seguridad de información en unidad NAS,» Putamayo, 2022.

[6] V. E. Rodriguez Arboleda, «Elaboración de una política de seguridad de la información para una institución pública basado en el esquema gubernamental de seguridad de la información,» Universidad Internacional SEK, 2018.

[7] C. N. S. C. S. B. J. C. F. S. Z. Rodrigo Arturo Proaño Escalante, «Sistemas basados en conocimiento como herramienta de ayuda en la auditoría de sistemas de información,» Quito, 2017.

[8] S. I. P. CORTEZ, «LA AUDITORÍA INTERNA COMO HERRAMIENTA DE GESTIÓN EN LAS EMPRESAS PÚBLICAS DE LA CIUDAD DE ESMERALDAS.,» 2018.

[9] D. X. Reascos Velastegui, « Auditoría informática al Departamento de Tecnología de la Información y Comunicación del Hospital Provincial General Docente Riobamba,» Riobamba, 2019.

[10] C. P. P. H. Jhony Zavala, «Auditoría informática al sistema contable y su incidencia en la confiabilidad de la información financiera, empresa CODIHE-S.A, período 2018.,» Riobamba, 2021.

[11] J. C. P. M. M. S. G. L. L. V. C. Silvia Edith Albarrán Trujillo, «Las Metodologías de la Auditoría Informática y su relación con Buenas Prácticas y Estándares,» Estado de México, 2020.

[12] E. A. O. Poloche, «Publicación: Desarrollo de un módulo integrado en el ITSM Gesthor® para el monitoreo, operación y conformidad con las Normas ISO 27001:2022 e ISO 20000:2018,» Bogotá, 2023.

[13] J. F. C. D. O. R. A. L. ROMERO, «IMPLEMENTACIÓN DE LA NORMA ISO 27001 PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ORIENTADA A LAS OFICINAS DE REGISTRO Y CONTROL ACADÉMICO, DIVISIÓN ADMINISTRATIVA Y FINANCIERA Y DE GESTIÓN TIC DE LA UNIVERSIDAD POPULAR DEL CESAR SECCIONAL AGUACHICA.,» 2021.

[14] J. G. Moya, «La importancia de la seguridad informática en la educación digital,» Quito, 2023.

[15] J. F. Córdoba Perdomo, «Diseño de un sistema automatizado de gestión de la seguridad de la información basado en la Norma ISO/IEC 27001:2013 para dar cumplimiento a la Ley 1581 de 2012 de protección de datos personales en el departamento de sistemas de una institución universita,» 2021.

[16] J. A. García Remache, «Diseño de un Sistema Integrado de Gestión basado en las normas ISO 9001:2015 e ISO 27001:2013, para la emisión de documentos de identificación militar en la matriz de la Dirección de Movilización del Comando Conjunto de las Fuerzas Armadas,» Quito, 2020.

[17] W. G. Montoya Martin, «Modelo guía para la Certificación en ISO 27001 de las entidades, que han implementado las normas establecidas por la estrategia de gobierno en línea.,» 2018.

[18] C. R. Gutiérrez, «Propuesta de implementación de un sistema de gestión de seguridad de la información aplicando la Norma ISO 27001:2013 para una institución del Estado en la Provincia Constitucional de Callao - 2021,» 2021.

[19] L. P. Á. Pampa Chacchi Jesús, «La tecnología de seguridad física y el sistema de seguridad en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2020,» Escuela Militar de Chorrillos Coronel Francisco Bolognesi, 2020.

[20] J. P. A. Salcedo Diaz, «Especificación de un método que ayude al banco popular a identificar y disminuir la brecha de seguridad de su software antivirus,» 2022.

[21] A. Postigo, «Seguridad Informática,» 2020.

[22] N. R. Niño Morante, «Modelo de un sistema de gestión de seguridad de información – SGSI, para fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información para el Instituto Nacional de Estadística e Informática - INEI filial Lambayeque,» 2019.

[23] A. M. Nieto Arias, «Sistema electrónico para la seguridad física, monitoreo y control de acceso para la empresa TSA S.A.,» 2019.

[24] D. M. T. Pérez, «Administración y seguridad: En redes de computadoras,» 2018.

[25] T. T. Lopez, «Clasificación de redes complejas usando funciones de caracterización que permitan discriminar entre redes aleatorias, Power-Law y Exponenciales,» 2007.

[26] M. D. J. P. Rodriguez Rodriguez Carlos Eduardo, «Evaluación del control de acceso en la red corporativa de la empresa Datum Ingenieria,» 2015.

[27] O. A. M. F. Hidalgo Jácome Mauricio Rafael, «Aplicación de una auditoría informática a la seguridad física a los equipos de cómputo del GAD municipal del cantón Salcedo ubicado en la provincia de Cotopaxi durante el periodo 2011,» Latacunga, 2014.

[28] E. A. Maya Olalla, «Auditoría de seguridad informática en la red interna de la Universidad Politécnica estatal del Carchi, basada en la Norma ISO/IEC 27001 y la metodología OSSTMMV3,» 2019.

[29] C. C. Hernández Obando, « Estudio de la seguridad en big data, privacidad y protección de datos mediante la ISO/IEC 27007:2017- aplicado a los datos académicos de la Universidad Técnica del Norte,» 2019.

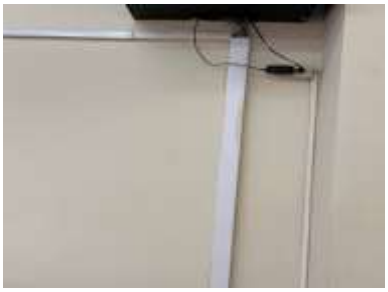
[30] M. P. B. M. ÁLAVA MERO CRISTIAN JOSÉ, «APLICACIÓN DE HACKING ÉTICO PARA LA DETERMINACIÓN DE AMENAZAS, RIESGOS Y VULNERABILIDADES EN LA RED WIFI DE LA UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ,» 2021.

ANEXOS

Anexo 1
Cronograma Detallado

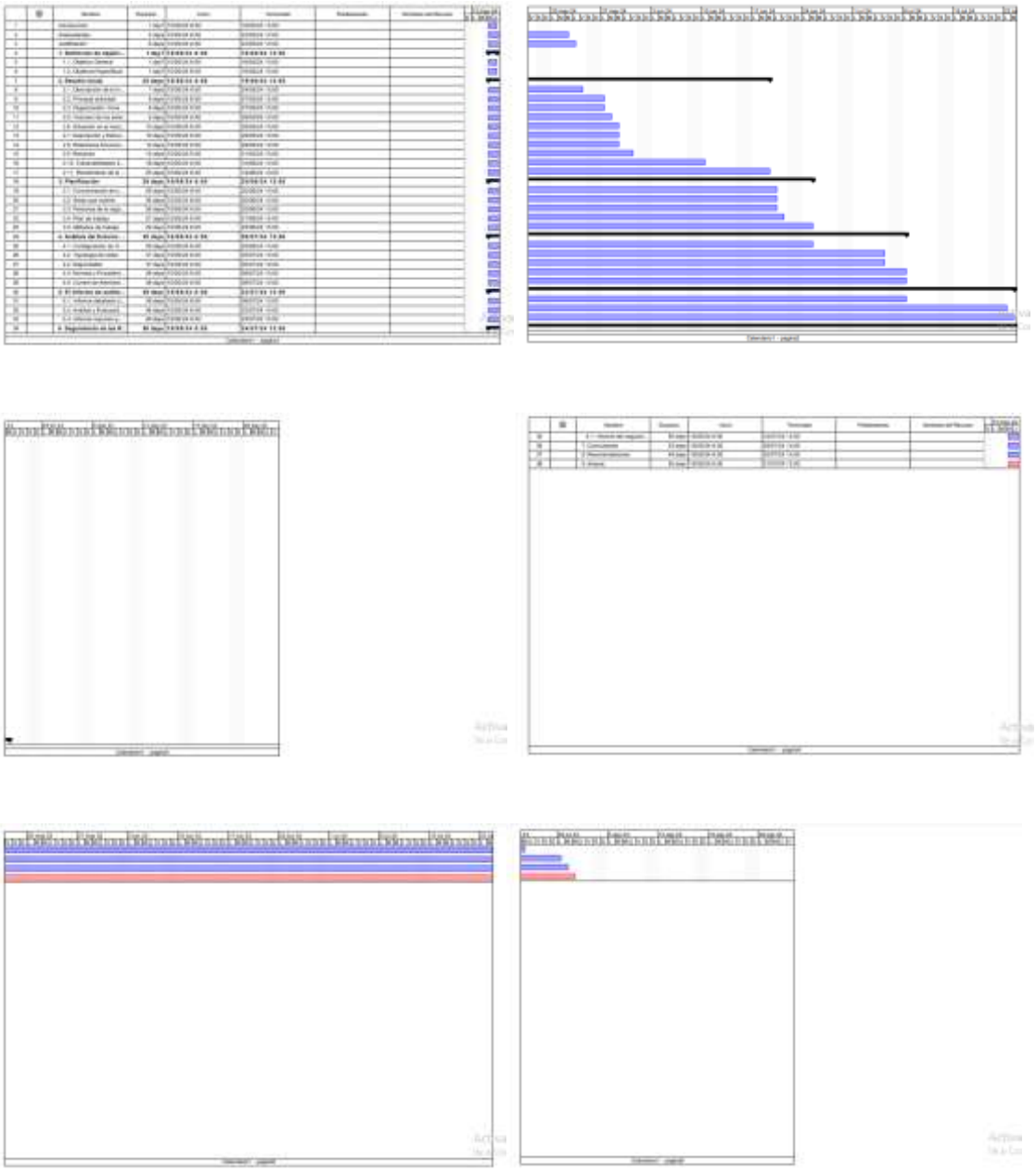
Actividad	Duración	Semana
Identificación de áreas críticas	2 semanas	Semana 1-2
Evaluación de controles de acceso	2 semanas	Semana 3-4
Protección contra desastres	2 semanas	Semana 5-6
Evaluación de la seguridad de los equipos	2 semanas	Semana 7-8
Revisión de procedimientos y políticas	2 semanas	Semana 9-10
Realización de pruebas y auditoría	2 semanas	Semana 11-12
Documentación y entrega de resultados	2 semanas	Semana 13-14

Anexo 2
Fotografías



Anexo 3

Calendario



Anexo 4: Matriz de evaluación de equipos del BLOQUE A

https://docs.google.com/spreadsheets/d/1ltsj3lSXhHE5u2hs08ocBFoyZLlR93AR/edit?usp=sharing&ouid=109870321505141777958&rtpof=true&sd=true

Anexo 5: Evaluación del plan de contingencia

resultado_encuestas (2).xlsx

Anexo 6: informe completo de vulnerabilidades de la Vlan 1:
report-c98ef48d-dad4-4feb-bae4-f75143e8e04b.pdf

Anexo 7: informe completo de vulnerabilidades de la Vlan 2:
report-9119ff02-5496-4977-ad1b-0200d6bc472e.pdf

Anexo 8: políticas de seguridad:
Políticas de Seguridad de la Información UNACHv2.pdf

Anexo 9: Cuestionario de Seguridad:
Cuestionario de SEGURIDAD-s.pdf

Anexo 10: Manual de Descripción, Valoración y Clasificación de Puestos:
https://www.unach.edu.ec/images/reglamentos/Manuales/2022/MANUAL%20DE%20DVC%20DE%20PUESTOS%20UNACH%20CODIFICADO%20A%20DICIEMBRE2021-signed.pdf

Anexo 11: Firewall:
FIREWALL.png

Anexo 12: Sistema de Gestión de la Red:
Juniper mist.png

Anexo 13: Reporte Semanal de Alertas:
Reporte semanal UNACH-2024-06-16-0238-0500_36825.pdf

Anexo 14: Infraestructura de Red:
UNACH-PGA-04-02-INFRAESTRUCTURA DE REDES.docx