REPÚBLICA DEL ECUADOR

TECNOLOGÍA SUPERIOR EN DESARROLLO DE SOFTWARE

IMPLEMENTACIÓN DE ESTRATEGIAS DE SEGURIDAD FÍSICA EN EL LABORATORIO DE CÓMPUTO DEL INSTITUTO SUPERIOR TECNOLÓGICO TENA

Trabajo de Integración Curricular, presentado como requisito parcial para optar por el título de Tecnólogo Superior en Desarrollo de Software.

AUTOR: JONATHAN ANDRES CHAVEZ PINDOLEMA

AUTOR: KAY ZACK TAPUY TANGUILA

TUTOR ING. FERNANDO NÚÑEZ C. MG.

Tena-Ecuador

2024-IS

APROBACIÓN DEL TUTOR

ING. FERNANDO NUÑEZ C. MG.

DOCENTE DEL INSTITUTO SUPERIOR TECNOLÓGICO TENA.

CERTIFICA:

En calidad de Tutor del Trabajo de Integración Curricular denominado, **IMPLEMENTACION DE ESTRATEGIAS DE SEGURIDAD FISICA EN EL LABORATORIO DE COMPUTO DEL INSTITUTO SUPERIOR TECNOLOGICO TENA**, de autoría de los señores Jonathan Andres Chavez Pindolema, con CC. 1550174344, Kay Zack Tapuy Tanguila con CC. 1550201808 estudiantes de la Carrera de Tecnología Superior en Desarrollo de Software del Instituto Superior Tecnológico Tena, **CERTIFICO que se ha realizado la revisión prolija del Trabajo antes citado, cumple con los requisitos de fondo y de forma que exige el respectivo reglamento institucional.**

Tena, 22 de agosto de 2024

Firmado electrónicamente por:
DARWIN FERNANDO
NUÑEZ COLLANTES

MG.TUTOR

ING. FERNANDO NUÑEZ C.

CERTIFICACIÓN DEL TRIBUNAL CALIFICADOR

Tena, 25 de agosto de 2024

Los Miembros del Tribunal de Grado abajo firmantes, certificamos que el Trabajo de Titulación denominado: IMPLEMENTACION DE ESTRATEGIAS DE SEGURIDAD FISICA EN EL LABORATORIO DE COMPUTO DEL INSTITUTO SUPERIOR TECNOLOGICO TENA, presentado por **JONATHAN ANDRES CHAVEZ PINDOLEMA**, con C.C: 1550174344, **KAY ZACK TAPUY TANGUILA** con C.C: 1550201808 estudiantes de la Carrera de Tecnología Superior en Desarrollo de Software del Instituto Superior Tecnológico Tena, ha sido corregida y revisada; por lo que autorizamos su presentación.

Atentamente,

Ing. Fausto Claudio
PRESIDENTE DEL
TRIBUNAL

Ing. Oswaldo Bonifaz
MIEMBRO DEL
TRIBUNAL

Ing. Martha Duarte
MIEMBRO DEL
TRIBUNAL

AUTORÍA

Nosotros, **JONATHAN ANDRES CHAVEZ PINDOLEMA**, con CC: 1550174344, **KAY ZACK TAPUY TANGUILA** con CC: 1550201808 declaramos ser autores del presente Trabajo de Titulación denominado: IMPLEMENTACION DE ESTRATEGIAS DE SEGURIDAD FISICA EN EL LABORATORIO DE COMPUTO DEL INSTITUTO SUPERIOR TECNOLOGICO TENA y absuelvo expresamente al Instituto Superior Tecnológico Tena, y a sus representantes jurídicos de posibles reclamos o acciones legales por el contenido de la misma.

Adicionalmente acepto y autorizo al Instituto Superior Tecnológico Tena, la publicación de mi trabajo de Titulación en el repositorio institucional- biblioteca Virtual.

AUTORES:

JONATHAN ANDRES CHAVEZ PINDOLEMACÉDULA: 155017434-4

KAY ZACK TAPUY TANGUILACÉDULA: 1550201808

FECHA: Tena, 25 de agosto de 2024

CARTA DE AUTORIZACIÓN POR PARTE DEL AUTOR

Nosotros, **JONATHAN ANDRES CHAVEZ PINDOLEMA, KAY ZACK TAPUY TANGUILA,** declaramos ser autores del Trabajo de Titulación titulado: **IMPLEMENTACION DE ESTRATEGIAS DE SEGURIDAD FISICA EN EL LABORATORIO DE COMPUTO DEL LABORATORIO DEL INSTITUTO SUPERIOR TECNOLOGICO TENA,** como requisito para la obtención del Título de: **TECNOLOGÍA SUPERIOR EN DESARROLLO DE SOFTWARE**; autorizo al Sistema Bibliotecario del Instituto Superior Tecnológico Tena, para que, con fines académicos, muestreal mundo la producción intelectual del Instituto, a través de la visualización de su contenido que constará en el Repositorio Digital Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el RDI, en las redes de información del país y del exterior, con las cuales tenga convenio el Instituto. El Instituto Superior Tecnológico Tena, no se responsabilizará por la copia o falsificación que de este trabajo que realice un tercero. Para constancia de esta autorización, en la ciudad de Tena, a los25 días del mes de agosto de 2024, firma el autor.

AUTOR: Jonathan Andres Chávez Pindolema
FIRMA:
CÉDULA: 155017434-4
DIRECCIÓN: Calle 5 – Barrio 3 de mayo
CORREO ELECTRÓNICO: jonathan.chavez@est.istt.terna.edu.ec
CELULAR: 0986808409

AUTOR: Kay Zack Tapuy Tanguila
FIRMA:
CÉDULA: 1550201808
DIRECCIÓN: Vía perimetral – Barrio paushiyacu
CORREO ELECTRÓNICO:
kay.tapuy@est.istt.terna.edu.ec**CELULAR**: 0969093078

DATOS COMPLEMENTARIOS

TUTOR: Ing. Fernando Núñez

TRIBUNAL DE GRADO:

Ing. Fausto Claudio (Presidente).

Ing. Oswaldo Bonifaz (Miembro).

Ing. Martha Duarte (Miembro).

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

DEDICATORIA

Dedico esta tesis a Dios, quien ha sido mi guía y fortaleza en cada paso de este camino,
ayudándome a superar los desafíos y a alcanzar mis metas.

A mi familia, por su amor incondicional, apoyo y por siempre estar a mi lado con sus palabrasde aliento y sabias enseñanzas, las cuales me han hecho crecer como persona y seguir adelante con determinación.

Autor: Jonathan Chavez.

AGRADECIMIENTO

Este informe está dedicado a mis padres, abuelos y amigos cercanos, quienes, con su apoyo,
motivación y constante guía han hecho posible este logro.

Agradezco profundamente a mi mejor amigo Steven Ontaneda, mis abuelos y nuevamente pormis padres por su valiosa colaboración, conocimientos compartidos y paciencia durante todoeste proceso. Sin su esfuerzo y dedicación, este proyecto no habría sido posible.

Así mismo agradecer al Instituto Superior Tecnológico Tena por permitirme formar parte desu noble educación que los profesores de la misma me han mostrado a lo largo de mis
estudios para cumplir mis objetivos.

Autor: Zack Tapuy

A. TEMA

IMPLEMENTACIÓN DE ESTRATEGIAS DE SEGURIDAD FÍSICA EN EL LABORATORIO DE CÓMPUTO DEL INSTITUTO SUPERIOR TECNOLÓGICO TENA

B. RESUMEN

Implementar estrategias de seguridad física en el laboratorio de cómputo del InstitutoSuperior Tecnológico Tena es crucial para proteger tanto los equipos como la información ylas personas que utilizan estas instalaciones. Entre las medidas esenciales se incluyen el control de acceso mediante sistemas de tarjetas de identificación, biometría o contraseñas, garantizando que solo el personal autorizado pueda ingresar al laboratorio. Además, la instalación de cámaras de seguridad y sistemas de vigilancia permite monitorear continuamente el área, previniendo robos y detectando actividades sospechosas. La protección física de los equipos, mediante cerraduras, soportes de seguridad y gabinetes, es fundamental para evitar su robo o daño. También es necesario realizar inspecciones periódicas de todos los sistemas de seguridad para asegurar su correcto funcionamiento y detectar posibles vulnerabilidades. La capacitación de personal y estudiantes en políticas de seguridad es esencial para que todos los usuarios comprendan la importancia de seguir los protocolos establecidos. Finalmente, contar con planes de emergencia bien definidos para responder a situaciones como incendios, robos o desastres naturales asegura que todos sepan cómo actuar en caso de un incidente. Estas estrategias no solo protegen los recursos físicos ytecnológicos del laboratorio, sino que también fomentan un ambiente seguro y confiable para la comunidad educativa del Instituto Superior Tecnológico Tena.

Palabras clave: Implementar, Seguridad, Robo, Control.

ABSTRACT

Implementing physical security strategies in the computer lab at Institute Superior Technologic Tena is crucial to protect both the equipment and the information and the people who use these facilities. Essential measures include access control through identification card systems, biometrics or passwords, ensuring that only authorized personnel can enter the laboratory. In addition, the installation of security cameras and surveillance systems allows for continuous monitoring of the area, preventing theft and detecting suspicious activities. Physical protection of the equipment, through locks, security brackets and cabinets, is essential to prevent theft or damage. Periodic inspections of all security systems are also necessary to ensure their proper functioning and detect possible vulnerabilities. Training of staff and students in security policies is essential so that all users understand the importanceof following established protocols. Finally, having well-defined emergency plans to respondto situations such as fires, theft or natural disasters ensures that everyone knows how to act in the event of an incident. These strategies not only protect the laboratory's physical and technological resources, but also foster a safe and secure environment for the educational community of the Institute Superior Technologic Tena.

Keywords: Implement, Security, Theft, and Control.

Reviewed by

Lcda. Belgica Gomez
Teacher of Languaje Center of IST TENA.

C. FUNDAMENTACIÓN DEL TEMA

1. Necesidad

El laboratorio de cómputo del Instituto Superior Tecnológico Tena es un espacio fundamentalpara el proceso educativo de los estudiantes, ya que ofrece acceso a recursos tecnológicos avanzados que facilitan el aprendizaje, la investigación y el desarrollo de habilidades prácticas. Este laboratorio está equipado con computadoras, servidores, dispositivos de almacenamiento y software especializado que son esenciales para la formación académica en diversas disciplinas, especialmente en aquellas relacionadas con la informática, la ingeniería y las ciencias aplicadas.

A pesar de la importancia de estos recursos, la infraestructura actual del laboratorio presenta deficiencias en términos de seguridad física. Estas deficiencias incluyen la falta de control efectivo sobre el acceso al laboratorio, la ausencia de barreras físicas robustas en áreas vulnerables como las ventanas, y la carencia de sistemas tecnológicos avanzados para monitorear y proteger el entorno. En este contexto, los equipos y recursos tecnológicos están expuestos a una serie de riesgos que pueden comprometer tanto la seguridad de los activos como la continuidad de las actividades académicas.

Uno de los principales riesgos es el robo de equipos, que no solo representa una pérdida económica significativa para la institución, sino que también puede interrumpir el desarrollo académico de los estudiantes, ya que la reposición de equipos costosos y especializados puedetomar tiempo. Además, la sustracción de equipos que contienen información sensible o proyectos en curso podría tener consecuencias graves en términos de pérdida de datos y violación de la privacidad.

2. Actualidad

En la actualidad, la seguridad física en entornos educativos, especialmente en áreas críticas como los laboratorios de cómputo, ha adquirido una relevancia sin precedentes. Con el rápido avance de la tecnología y la creciente dependencia de los recursos digitales en la

educación, las instituciones académicas han experimentado un aumento en los incidentes de seguridad queponen en riesgo no solo los equipos y datos, sino también la continuidad de las actividades educativas.

A nivel global, muchas instituciones educativas han sido objeto de robos de equipos tecnológicos, intrusiones no autorizadas y actos de vandalismo, lo que ha generado una creciente preocupación por la protección de estos activos. Este fenómeno no es ajeno al Instituto Superior Tecnológico Tena, donde la infraestructura tecnológica es un pilar fundamental para la formación académica de los estudiantes. En un entorno donde los recursoseconómicos son limitados y la reposición de equipos costosos es un desafío, la seguridad físicase convierte en una prioridad estratégica para asegurar la continuidad operativa y académica del laboratorio de cómputo.

Además, el contexto actual se ve influenciado por la transformación digital y el aumento del uso de dispositivos móviles y portátiles, lo que ha incrementado el valor de los activos tecnológicos en los laboratorios. Estos dispositivos no solo son valiosos en términos monetarios, sino también en términos de la información que contienen. Proyectos de investigación, trabajos académicos, datos sensibles y software especializado están almacenados en estos equipos, lo que hace que cualquier pérdida o daño tenga un impacto significativo en la misión educativa de la institución.

3. Importancia

La importancia de implementar estrategias de seguridad física en el laboratorio de cómputo del Instituto Superior Tecnológico Tena radica en varios aspectos fundamentales que impactantanto en el desarrollo académico como en la gestión institucional. En un contexto educativo donde la tecnología juega un papel

central, garantizar la protección de los recursostecnológicos se convierte en una prioridad que afecta directamente la calidad del aprendizaje,la continuidad de las actividades académicas, y la reputación de la institución.

Protección de Activos Tecnológicos

El laboratorio de cómputo alberga equipos costosos y especializados, como computadoras, servidores, dispositivos de almacenamiento, y software con licencias valiosas. Estos activos no solo representan una inversión económica significativa, sino que también son herramientasesenciales para el aprendizaje, la investigación y la innovación. La pérdida o daño de estos recursos, debido a incidentes de seguridad como robos o vandalismo, podría paralizar las actividades académicas, retrasar proyectos de investigación y generar costos elevados para la institución, tanto en términos de reposición de equipos como de interrupción de servicios educativos.

4. Presentación del problema profesional a responder

El problema central que se aborda es la vulnerabilidad del laboratorio de cómputo frente a incidentes de seguridad que podrían comprometer los recursos tecnológicos y la integridad del entorno académico. La falta de medidas de seguridad física adecuadaspone en riesgo tanto los equipos como la información almacenada en ellos, lo que podría tener consecuencias negativas en el desarrollo académico y operativo del instituto.

Campo: El problema se sitúa en el campo de la seguridad física dentro del entorno educativo, un área que se enfoca en la protección de recursos tangibles, como equipos tecnológicos y las infraestructuras que los albergan, para garantizar la integridad y continuidad de las actividades

académicas.

Área: Dentro del área de gestión de infraestructura educativa, el desafío radica en implementar medidas de seguridad adecuadas que protejan los activos tecnológicos del laboratorio de cómputo. Este laboratorio es crucial para el aprendizaje de los estudiantes, y su vulnerabilidad ante robos, vandalismo y accesos no autorizados representa una amenaza directa a la calidad educativa y la eficiencia operativa de la institución.

Aspecto: El aspecto central del problema se refiere a la insuficiencia de estrategias de seguridad física que aseguren el acceso controlado y la protección física de los equipos. Actualmente, la falta de controles estrictos sobre quiénes pueden ingresar al laboratorio, junto con la debilidad de las barreras físicas existentes, pone en riesgo tanto los equipos como la información sensible que contienen.

Sector: Este problema se ubica en el sector de la educación superior tecnológica, donde la seguridad de los recursos académicos es fundamental para el desarrollo de las capacidades de los estudiantes y la reputación de la institución. En particular, el Instituto Superior Tecnológico Tena, al ser una entidad que forma profesionales en áreas técnicas, debe asegurar que sus laboratorios de cómputo estén protegidos contra cualquier tipo de amenaza física.

Línea de Investigación: La investigación se orienta hacia el diseño e implementaciónde estrategias de seguridad física eficaces en entornos académicos tecnológicos. Esta línea de investigación busca identificar las mejores prácticas y tecnologías disponibles, como el uso de sistemas

biométricos y barreras físicas, que puedan integrarse de manera eficiente en el entorno del laboratorio de cómputo para garantizar su protecciónyla continuidad de las actividades educativas.

5. Delimitación

5.1. Delimitación Espacial

El Trabajo de Integración Curricular se realizó en el Instituto Superior Tecnológico Tena, El mismo que está ubicado en la vía Tena-Archidona en el km 1.5 provincia de napo.

5.2. Delimitación Temporal

El proyecto de lo efectuara en el Periodo Académico 2024-IS

5.3. Delimitación Técnica

La implementación incluyó la instalación de un sistema de acceso biométrico en la entrada del laboratorio y la colocación de rejas de seguridad en la parte inferior de las ventanas. Estos sistemas serán seleccionados de acuerdo a estándares de calidady eficacia reconocidos en el ámbito de la seguridad física.

6. Unidades de información

Las unidades de observación que se contemplan para este trabajo están enfocadas directamente a la Unidad de TIC del Instituto Superior Tecnológico Tena. Estas unidades de observación proporcionan una base sólida para el análisis del problema y para la formulación de estrategias de seguridad física que sean efectivas y sostenibles en el tiempo,asegurando así la protección del laboratorio de cómputo del Instituto Superior Tecnológico Tena.

7. Beneficiarios

7.1. Directos

- Instituto Superior Tecnológico Tena

7.2. Indirectos

- Personal Administrativo
- Docentes
- Estudiantes

D. OBJETIVOS

1. Objetivo General

Implementar estrategias de seguridad física en el laboratorio de cómputo del InstitutoSuperior Tecnológico Tena.

2. Objetivos Específicos

- Evaluar las condiciones actuales de seguridad física del laboratorio de computación, identificando áreas vulnerables, riesgos potenciales y necesidades específicas de protección.
- Establecer protocolos de seguridad física para prevenir y mitigar riesgos antrópicos que puedan afectar la integridad del laboratorio y sus componentes.
- Capacitar y concientizar al personal docente, administrativo y estudiantil sobre las medidas de seguridad física implementadas, promoviendo prácticas y comportamientos seguros dentro del laboratorio de computación.

E. ASIGNATURAS INTEGRADORAS

Tabla 1: Asignaturas integradoras

Asignaturas	Resultados de Aprendizaje
Fundamentos de redes y conectividad	Aplica conceptos y definiciones de los fundamentos de redes para comunicar dispositivos.
Análisis y Diseño de Sistemas	Aplica metodologías y técnicas de investigación en la búsqueda, fundamentación y elaboración de soluciones informáticas.
Metodologías al Desarrollo de Software	Identifica oportunidades para mejorar eldesempeño de las organizaciones a través del uso eficiente y eficaz de soluciones informáticas.

F. FUNDAMENTACIÓN TEÓRICA

- **Conceptos de Seguridad Física**

La seguridad física abarca una serie de medidas y controles diseñados para salvaguardar recursos tangibles, como edificios, instalaciones, equipos y personal, frente a diversas amenazas. Estas amenazas pueden incluir acceso no autorizado, robos, actos de vandalismo, desastres naturales, entre otros incidentes que podrían comprometer la integridad de estos recursos. Entre las medidas más comunes se encuentran los sistemas de control de acceso, la vigilancia, la protección contra incendios, y los sistemas de detección de

intrusos. (Fennelly & Perry, 2016)

La seguridad física se basa en tres principios fundamentales: la disuasión, la detección y la respuesta. La disuasión se logra mediante la implementación de medidas visibles y eficaces que desalienten a los posibles infractores. La detección implica la capacidad de identificar y monitorear actividades sospechosas o no autorizadas. Por último,la respuesta se refiere a las acciones coordinadas y oportunas para mitigar y resolver los incidentes de seguridad.

- **Importancia de la Seguridad Física en Laboratorios de Computación**

Los laboratorios de computación son entornos críticos que albergan recursos tecnológicos valiosos, equipos informáticos costosos y datos sensibles. Por lo tanto, la implementación de medidas de seguridad física adecuadas es fundamental por varias razones:

- **Protección de activos:** Los equipos informáticos, servidores, dispositivos de almacenamiento y otros recursos tecnológicos representan una inversión significativa para la institución. La seguridad física ayuda a proteger estos activos contra el robo, el vandalismo y el daño accidental. (Fennelly & Perry, 2016)
- **Salvaguardar la información:** Los laboratorios de computación almacenan y procesan información confidencial, como datos personales, resultados de investigaciones e información académica privilegiada. La seguridad física ayuda prevenir el acceso no autorizado y la fuga de datos sensibles. (Fennelly & Perry, 2016)
- **Continuidad de operaciones:** Un incidente de seguridad física,

como un robo o un ataque, puede interrumpir las actividades académicas y de investigación en el laboratorio. Las medidas de seguridad adecuadas garantizan la continuidad de lasoperaciones y minimizan las disrupciones. (Fennelly & Perry, 2016)

- **Cumplimiento normativo:** Existen regulaciones y estándares específicos que las instituciones educativas deben cumplir en materia de seguridad física y

  protección de datos. La implementación de un plan de seguridad física sólido ayuda a cumplir con estas normativas. (ISO & IEC, 2022)

- **Protección del personal y los estudiantes:** Un entorno seguro y controlado en ellaboratorio de computación protege la integridad física de los estudiantes y el personal, evitando posibles incidentes o accidentes. (ISO/IEC, 2022)

- **Normativas y Estándares Aplicables**

Existen varias normativas y estándares internacionales que establecen los requisitos y mejores prácticas en materia de seguridad física para instalaciones y entornos tecnológicos. Algunas de las más relevantes son: ISO/IEC 27001 - Sistema de Gestión de Seguridad de la Información

La norma ISO/IEC 27001 es una norma internacional que establece los requisitos para unsistema de gestión de seguridad de la información (SGSI). Este estándar proporciona un enfoque sistemático para gestionar la información sensible de la empresa, garantizando su seguridad y confiabilidad. (ISO & IEC, 2022)

i. **Política de Seguridad de la Información**: Definición de una política formal de seguridad que describa la dirección y el apoyo de la gestión. (ISO & IEC, 2022)

ii. **Análisis de Riesgos**: Identificación de los riesgos que pueden afectar a la información y la implementación de controles para mitigarlos. (ISO & IEC, 2022)

iii. **Controles de Seguridad**: Establecimiento de medidas y controles para proteger la información, que pueden incluir desde contraseñas hastamedidas físicas como cerraduras y cámaras de seguridad. (ISO & IEC, 2022)

- **Revisión y Mejora Continua**

Evaluación regular del SGSI y mejoras basadas en los resultados de auditorías y revisiones.

Beneficios:

i. Mejora la gestión y protección de la información.

ii. Aumenta la confianza de clientes y socios.

iii. Cumple con requisitos legales y regulatorios.

iv. Reducción del impacto de incidentes de seguridad.

- **NIST SP 800-53 - Controles de Seguridad y Privacidad para Sistemas de InformaciónFederales**

El NIST SP 800-53 es una publicación del Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos. Ofrece una guía exhaustiva sobre controles de seguridad y privacidad, incluyendo controles físicos, para sistemas de información federales (National Institute of Standards and Technology [NIST], 2020).

i. Categorías de Controles: Los controles se agrupan en familias como acceso y control de cuentas, protección de la información y

comunicaciones, y seguridadfísica y ambiental.

ii. Selección y Especificación de Controles: Proceso para seleccionar y especificarcontroles basados en el impacto potencial de la pérdida de confidencialidad, integridad y disponibilidad de la información.

iii. Implementación y Evaluación: Guía sobre cómo implementar y evaluar la efectividad de los controles de seguridad.

Beneficios:

iv. Proporciona una estructura para asegurar sistemas de información.

v. Ayuda a cumplir con los requisitos federales de seguridad.

vi. Mejora la gestión de riesgos de seguridad y privacidad.

- **COBIT 5 - Marco de Gobierno y Gestión de TI**

COBIT 5, desarrollado por ISACA, es un marco integral para el gobierno y la gestión de las tecnologías de la información (TI). Ofrece principios, prácticas, herramientas y modelos para la gobernanza de TI, incluyendo aspectos de seguridadfísica. (ISACA, 2012)

i. **Principios de Gobernanza**: COBIT 5 se basa en principios como satisfacer las necesidades de los stakeholders, cubrir la organización de extremo a extremo, aplicar un enfoque integral, habilitar un enfoque holístico y separar la gobernanza de la gestión. (ISACA, 2012)

ii. **Modelo de Referencia de Procesos**: Define un modelo de referencia de procesos que cubre la gobernanza y la gestión de TI. (ISACA, 2012)

iii. **Habilitadores de Gobernanza y Gestión**: Identifica siete

categorías de habilitadores que influyen en la gobernanza y la gestión de TI, incluyendoprincipios, políticas y marcos; procesos; estructuras organizacionales; cultura, ética y comportamiento; información; servicios, infraestructura y aplicaciones; y personas, habilidades y competencias. (ISACA, 2012)

iv. Facilita la alineación de la TI con los objetivos de negocio.

v. Mejora la eficiencia y efectividad de la TI.

vi. Reduce riesgos y optimiza recursos.

- **ISO/IEC 27002 - Código de Prácticas para Controles de Seguridad de la Información**

La norma ISO/IEC 27002 proporciona prácticas recomendadas para la implementación de controles de seguridad de la información y actúa como una guía complementariaa la ISO/IEC 27001. (ISO/IEC, 2022)

- **Selección de Controles**: Proporciona una lista de controles de seguridad quepueden seleccionarse e implementarse en función de los riesgos identificados.
- **Categorías de Controles**: Los controles se agrupan en diferentes categorías como políticas de seguridad, seguridad organizacional, seguridad de recursos humanos, gestión de activos, control de acceso, criptografía, seguridad física yambiental, entre otros.
- **Implementación y Gestión**: Guía sobre cómo implementar, gestionar y revisarlos controles de seguridad de manera efectiva.

Beneficios:

- Facilita la implementación de un SGSI basado en ISO/IEC 27001.

- Ayuda a proteger la información de manera integral.
- Proporciona un enfoque sistemático y probado para la seguridad de lainformación.

- **Regulaciones y normativas locales**

Dependiendo de la ubicación geográfica y el país, existen regulaciones y normas específicas establecidas por autoridades locales o nacionales que deben ser cumplidas para asegurar la protección de la información y la infraestructura.

- **Regulaciones Nacionales**: Pueden incluir leyes de protección de datos, como el Reglamento General de Protección de Datos (GDPR) en Europa, o la Ley de Privacidad del Consumidor de California (CCPA) en Estados Unidos. (European Parliament, & Council of the European Union, 2016)
- **Normativas Sectoriales**: Algunas industrias tienen regulaciones específicas, como la Ley de Portabilidad y Responsabilidad del Segurode Salud (HIPAA) para el sector de la salud en Estados Unidos (U.S. Department of Health & Human Services. 2013)
- **Estándares Locales**: Pueden existir estándares locales específicos para la seguridad física y la gestión de la información que complementan los estándares internacionales.

Beneficios:

- Cumplimiento con requisitos legales y regulatorios específicos.
- Mejora de la seguridad y protección de la información adaptada acontextos locales.
- Reducción del riesgo de sanciones legales y pérdida dereputación.

Es importante que el Instituto Superior Tecnológico Tena revise y cumpla con las normativas y estándares aplicables para garantizar la implementación efectiva de un plan de seguridad física sólido y alineado con las mejores prácticas internacionales.

- **COIP Artículos Referentes.**

Artículo 196.- Hurto. - La persona que, sin ejercer violencia, amenaza o intimidación en la persona o fuerza en las cosas, se apodere ilegítimamente de cosa mueble ajena, será sancionadacon pena privativa de libertad de seis meses a dos años. Si el delito se comete sobre bienes públicos se impondrá el máximo de la pena prevista aumentada en un tercio. Para la determinación de la pena se considerará el valor de la cosa al momento del apoderamiento.

Este artículo define el robo como la sustracción de bienes ajenos mediante el uso de fuerza en
las cosas o violencia en las personas. En el contexto de un laboratorio de cómputo, el robo de equipos tecnológicos podría ser sancionado bajo este artículo, y la implementación de medidasde seguridad física (como cámaras y controles de acceso) puede prevenir este tipo de delitos (Asamblea Nacional del Ecuador, 2014).

G. METODOLOGÍA

El siguiente capítulo se define de cómo se desarrolló el tema del proyecto Implementación De Estrategias De Seguridad Física En El Laboratorio De Cómputo Del Instituto Superior Tecnológico Tena.

1. Materiales

- Rejas de Acero Galvanizado
- Tornillo de anclaje
- Tacos de expansión
- Soporte de montaje
- Llave de impacto
- Cortadora de metal
- Guantes y equipo de protección personal (EPP)
- Batería
- Cables de conexión
- Pelacables
- Guantes
- Manuales

2. Equipos

- Una laptop (DELL)
- Taladro
- Multímetro
- Sistema de control de acceso biométrico
- Cerradura electrónica

3. Ubicación del Área de estudio

La ubicación del área de estudio es el km 1.5 en la vía Tena-Archidona,

cantón Tena provincia de Napo en el Laboratorio de Cómputo del Instituto Superior Tecnológico Tena.

4. Tipo de investigación

El tipo de investigación que se llevó a cabo es de naturaleza aplicada y descriptiva:

- Investigación Aplicada: Busca la resolución de un problema específico, eneste caso, la mejora de la seguridad física del laboratorio de cómputo. El objetivo es desarrollar e implementar estrategias de seguridad que sean efectivas y sostenibles.
- Investigación Descriptiva: Se centra en describir las condiciones actuales del laboratorio, identificar las vulnerabilidades de seguridad existentes, y evaluar el impacto de las medidas de seguridad implementadas. Este tipo de investigación proporciona una visión detallada del entorno de estudio ylas soluciones propuestas.

5. Metodología para cada objetivo

5.1.Objetivo específico 1:

Evaluar las condiciones actuales de seguridad física del laboratorio de computación, identificando áreas vulnerables, riesgos potenciales y necesidades específicas de protección.

- **Evaluación de la Infraestructura Tecnológica:**

Se efectuó una visita en la cual se realizó la observación detallada de la infraestructurafísica del IST Tena, identificando activos críticos, sistemas de

seguridad los mismos que no cuentan con medidas de seguridad física adecuada.

- **Encuesta:**

Se realizó una encuesta a los estudiantes de la carrera de desarrollo de software del IST Tena para comprender las percepciones sobre la seguridad física y obtener informaciónsobre potenciales riesgos.

- **Análisis de Incidentes Anteriores:**

Se realizó una entrevista al coordinador de la carrera de desarrollo de software del IST Tena con la finalidad de conocer sobre los incidentes de seguridad anteriores, identificando las causas subyacentes, las lecciones aprendidas y las áreas de mejoras.

- **Revisión de la seguridad física del laboratorio:**

Se realizó una observación directa de cómo se encuentra el laboratorio de cómputo delIST Tena, con la finalidad de evaluar las medidas de seguridad del laboratorio como accesos físicos y la infraestructura del mismo, para asegurar la protección adecuada de los recursos tecnológicos.

5.2. Objetivo específico 2:

Establecer protocolos de seguridad física para prevenir y mitigar riesgos antrópicos quepuedan afectar la integridad del laboratorio y sus componentes. Según lasencuestas y la observación directa se enumeró una lista de estrategias de mitigación sobre la seguridad física del laboratorio de cómputo del IST Tena las cuales son:

- Implementación de controles de acceso físico (tarjetas, biométricos, etc.)
- Instalación de sistemas de vigilancia y monitoreo (cámaras, sensores, etc.)

- Desarrollo de protocolos de seguridad y planes de contingencia
- Programas de capacitación y concientización para el personal y los estudiantes
- Mejoras en la infraestructura física del laboratorio (reforzamiento de puertas,ventanas, etc.)

5.3. Objetivo específico 3:

Capacitar y concientizar al personal docente, administrativo y estudiantil sobre las medidas de seguridad física implementadas, promoviendo prácticas y comportamientos seguros dentro del laboratorio de computación.

Con la información obtenida del laboratorio se contrató a una persona capacitada en seguridad física el cual nos dio una gran charla y recomendaciones del laboratorio el cual nosayudó a implementar las medidas de seguridad en el laboratorio.

H. RESULTADOS

1. Resultados del objetivo 1

1.1. Observación directa

Dentro del laboratorio del Instituto Superior Tecnológico Tena se cuenta con:

1.1.1. Equipos y Protección Eléctrica:

- **Cantidad de computadoras:** El laboratorio cuenta con 38computadoras usables.
- **Protección eléctrica:** Las computadoras están conectadas a reguladoresde voltaje, pero no poseen UPS (Uninterruptible Power Supply).

Recomendación: Es recomendable instalar UPS para cada computadora o grupo de computadoras. Los UPS no solo regulan el voltaje, sino que también proporcionan energía temporal en caso de cortes eléctricos, permitiendo el correcto apagado de los equipos y previniendo daños por apagones bruscos.

1.1.2. Equipos de Emergencia y Seguridad:

- Botiquín: El laboratorio cuenta con un botiquín de primeros auxilios.

  Recomendación: Asegurarse de que el botiquín esté bien surtido y revisarperiódicamente la caducidad de los insumos.

- Extintor: Hay un extintor disponible en el laboratorio.

  Recomendación: Verificar que el extintor esté en buen estado y que serealicen inspecciones regulares para asegurarse de que esté operativo.

- Cámara de seguridad: El laboratorio tiene una cámara de seguridad.

  Recomendación: Evaluar la ubicación de la cámara para asegurar que cubra lasáreas críticas del laboratorio. Considerar la instalación de cámaras adicionales para una mejor cobertura.

- Sensores de humo: Existen 2 sensores de humo en el laboratorio.

  Recomendación: Realizar pruebas regulares para asegurar que los sensores funcionen correctamente y estén en lugares estratégicos para detectar cualquierincendio rápidamente.

1.1.3. Equipos Adicionales:

- Proyector: Hay un proyector en el laboratorio.
- Aire acondicionado: Dentro del laboratorio se contó 2 unidades de aireacondicionado.

Recomendación: Asegurarse de que los equipos de aire acondicionado reciban mantenimiento regular para evitar fallos que puedan afectar a los equipos de cómputo.

1.1.4. Seguridad Física del Laboratorio:

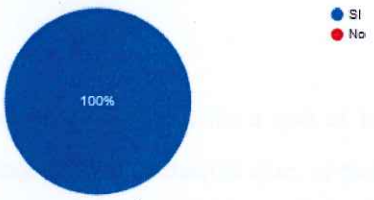
- Puerta de ingreso: La puerta de ingreso posee rejas, lo que proporciona unamedida de seguridad contra intrusos.
- Ventanas: Las ventanas no tienen rejas.

  Recomendación: Instalar rejas en las ventanas para prevenir robos y asegurar que el laboratorio esté protegido contra accesos no autorizados.

1.2. Encuesta

Pregunta 1 ¿Conoce usted el Laboratorio de Informática del Instituto Superior TecnológicoTena?

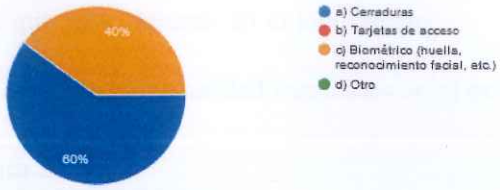
Figura 1: Pregunta 1



Interpretación: del 100% de los encuestados el 100% conoce que el IST Tena cuenta con unlaboratorio de cómputo y conoce la ubicación del mismo.

Pregunta 2 ¿Cuenta el laboratorio con un control de acceso (por ejemplo, cerraduras, tarjetasde acceso, biométrico, etc.)?

Figura 2: Pregunta 2



Interpretación: del 100% de los encuestados el 100% manifiesta que el laboratorio del IST Tena cuenta con un control de acceso.

Pregunta 3 ¿Si la respuesta anterior fue Sí, "qué tipo de control de acceso se utiliza?

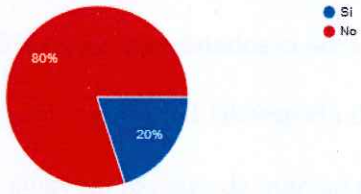
Figura 3: Pregunta 3

Interpretación: del 100% de los encuestados el 60% manifiesta que el laboratorio cuenta conel control de acceso de cerraduras, mientras que el 40% manifiesta que posee un control de acceso biométrico (huella, reconocimiento facial, etc.)

Nota: tras realizar una entrevista puesto a que el laboratorio no cuenta con un biométrico y enla encuesta respondieron que, si posee, acudimos a preguntar y nos respondieron que se confundieron por el cuarto de servidores.

Pregunta 4 ¿Hay cámaras de seguridad de seguridad en el laboratorio?

Figura 4: Pregunta 4

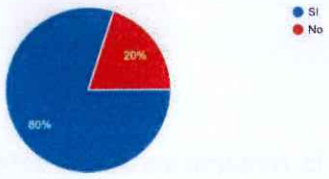


Interpretación: del 100% de los encuestados el 80% manifiestan que no, ya sea porque aun no han tenido la oportunidad de ingresar al laboratorio, mientras que

el 20% manifiesta que siha cámaras en el laboratorio.

Pregunta 5 ¿Hay cámaras de seguridad instaladas en el exterior del laboratorio?

Figura 5: Pregunta 5



Interpretación: Del 100% de los encuestados el 80% **del mismo** afirmaron que si existe la presencia de cámaras fuera del laboratorio del IST Tena, mientras que el 20% de los mismos rigieron lo contrario.

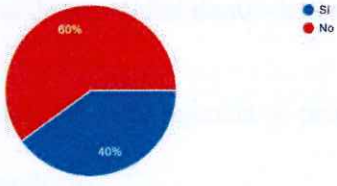
Pregunta 6 ¿Hay personal de seguridad que vigile el área del laboratorio?

Figura 6: Pregunta 6

Interpretación: del 100% de los encuestados el 80% manifiestan que, si hay personal de seguridad, pero no específicamente para el laboratorio del IST Tena sino también para otras áreas, mientras que el 20% manifiesta que si ha visto personal de seguridad específicamente para el laboratorio.

Pregunta 7 ¿Sacan un registro de las personas que ingresan al laboratorio?

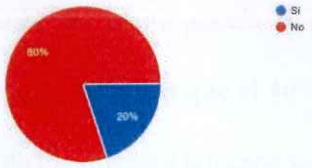
Figura 7: Pregunta 7



Interpretación: del 100% de los encuestados el 60% manifiestan que no hay un registro de las personas que ingresan al laboratorio del IST Tena, mientras que el 40% manifiestan que sihay un registro de ingreso al mismo.

Pregunta 8 ¿Hay procedimientos para la salida de equipos del laboratorio?

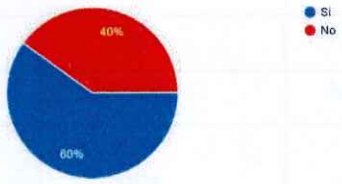
Figura 8: Pregunta 8



Interpretación: Del 100% de los encuestados el 80% manifiestan que no se realiza un procedimiento para la salida de equipos del laboratorio del IST Tena debe ser porque la mayoría que respondieron son estudiantes lo cuales no debieron ser capacitados sobre esa normativa, mientras que el 20% manifestó que si hay un procedimiento para la salida de un equipo del laboratorio.

Pregunta 9 ¿Hay sistemas de protección y protección contra incendios en el laboratorio?

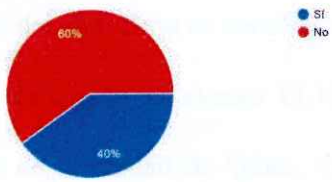
Figura 9: Pregunta 9



Interpretación: Del 100% de los encuestados el 60 % manifiesta que si se encuentran sistemasde protección contra incendios en el laboratorio como puede ser (sensor de humo, extintor, etc.), mientras que el 40% manifiesta que no se encuentra ningún sistema de seguridad dentrodel laboratorio.

Pregunta 10 ¿Hay planos de contingencia y procedimientos de emergencia establecidos para el laboratorio?

Figura 10: Pregunta 10



Interpretación: Del 100% de los encuestados el 60% manifiestan que no se encuentra o no hay planos de contingencia o procedimientos de emergencias establecidos en el laboratorio, mientras que el 40% manifiesta que si puesto que se ha hecho capacitaciones de los mismos almomento de ingresar al laboratorio.

2. Resultados del objetivo 2

Para desarrollar nuestro objetivo dos creamos una tabla donde evaluamos los riesgosseparando su probabilidad, impacto y midiendo el riesgo del mismo.

Tabla 2: Tabla en COBIT5

Riesgo	Probabilidad	Impacto	Nivel deRiesgo
Robo	Alta	Alto	Crítico
Acceso no autorizado	Media	Alto	Alto
Vandalismo	Baja	Medio	Medio
Fallo eléctrico	Media	Medio	Medio
Sabotaje interno	Baja	Alto	Medio
Ataques cibernéticos	Alta	Alto	Crítico
Errores humanos	Alta	Medio	Alto

Mediante las observaciones de nuestra tabla creamos un listado de estrategias de mitigaciónde riesgo físico para el laboratorio.

3. Resultados del objetivo 3

En función a la encuesta que se realizo a los estudiantes de la carrera de desarrollo de software del IST Tena se concluyo en los temas a abordar en la capacitación que se realizo en el evento FLISOL en colaboración de un ingeniero proveniente de la ciudad de Quito, quien dio a conocer sobre las

siguientes temáticas abordadas:

- **Seguridad física en entornos de TI:** Se discutió la importancia de proteger el laboratoriode riesgos físicos, como robos, sabotaje y otros daños.
- **Control de acceso al laboratorio:** Se revisaron las técnicas para limitar el acceso al personal autorizado, incluyendo el uso de credenciales, cámaras de seguridad y registrosde acceso.
- **Protección de equipos y activos del laboratorio:** Se explicaron medidas preventivas como el uso de candados, UPS, sistemas de monitoreo de temperatura y estrategias de mantenimiento preventivo.

➢ **Importancia del Registro de Asistencia:**

- El registro de asistencia permite llevar un control formal de los participantes.

Este archivo es vital para:

- Verificar la participación.
- Hacer un seguimiento sobre la efectividad de la capacitación.

Lo cual se evidencia en la figura 23 de anexos.

➢ **Resultados del taller**

- **Objetivos alcanzados:**
  - Se logró capacitar a los participantes sobre los riesgos y medidas de mitigación de la seguridad física en el laboratorio.
  - Se promovió el uso correcto del laboratorio, mejorando la conciencia sobre la importancia de la seguridad física.
- **Efectividad:** Una vez finalizada la capacitación se procedió a

solventar preguntas y/o dudas realizadas por los participantes, se confirmó que los participantes comprendieron los puntos clave discutidos lo cual fue muy satisfactorio para nuestro proyecto.

- **Puntos relevantes de la capacitación**

La experiencia del especialista proveniente de la ciudad de Quito aportó un enfoque técnico y práctico sobre las medidas de mitigación de seguridad física antrópica lo cual nos ayudó a la toma de decisiones para la implementación de las medidas de seguridad las cuales implementamos posterior a la capacitación.

- **Riesgos físicos identificados:** Se discutieron ejemplos reales de riesgos que podrían ocurrir en el laboratorio, sobrecarga eléctrica y acceso no autorizado.
- **Estrategias de mitigación:** Se propusieron soluciones, como la instalación de rejas al exterior del laboratorio, sistemas de control de acceso y mantenimiento regular de equipos

- **Conclusión**

La capacitación fue exitosa en generar conciencia y proveer herramientas útiles paramejorar la seguridad física del laboratorio. Los participantes demostraron una comprensión sólida de los conceptos discutidos.

I. CONCLUSIONES

- La implementación de estrategias de seguridad física, como la instalación de sistemas de control de acceso biométrico y el refuerzo de la infraestructura con rejasy puertas de seguridad, ha mejorado significativamente la protección de los recursos tecnológicos críticos del laboratorio. Esto no solo reduce el riesgo de robosy daños, sino que también garantiza un entorno más seguro para las actividades académicas.
- La capacitación y concientización del personal docente, administrativo y estudiantil sobre las medidas de seguridad física han contribuido a desarrollar una cultura de responsabilidad compartida.
- La realización de auditorías periódicas, junto con un programa de mantenimiento regular, asegura que las medidas de seguridad implementadas se mantengan efectivas y actualizadas.

J. RECOMENDACIONES

- Se recomienda desarrollar un programa regular de capacitación y concientización sobre seguridad para el personal docente, administrativo y estudiantil.
- Es esencial llevar a cabo auditorías de seguridad de manera regular para evaluar laefectividad de las estrategias implementadas.
- Se recomienda establecer un protocolo de respuesta rápida en caso de incidentes deseguridad, como robos o accesos no autorizados.

K. BIBLIOGRAFIA

Álvarez, J. M. (2020). *Seguridad física en entornos educativos: Estrategias y mejoresprácticas*. Editorial Académica Española.

Vásquez, L., & Espinoza, R. (2022). *Estrategias de seguridad física en laboratorios académicos: Un enfoque preventivo*. Revista de Tecnología y Seguridad, 13(1), 75-92.

Acosta, J., & Paredes, M. (2023). Evaluación de riesgos en laboratorios de informática: Unaguía práctica. Revista de Tecnología Educativa, 19(2), 45-59.

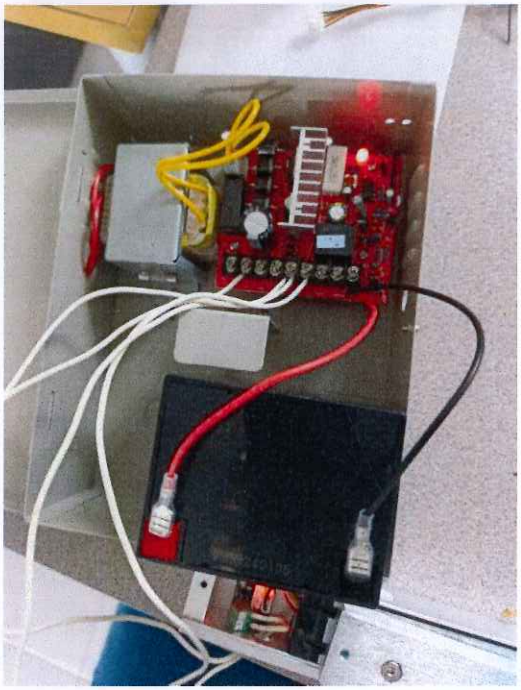
Barrera, L., & Flores, G. (2022). Diseño e implementación de sistemas de seguridad física en centros educativos. Journal of Educational Technology, 27(4), 112-129.

García, M., & Velasco, D. (2023). Estrategias de protección física en laboratorios de cómputo:Un estudio de caso. Revista Latinoamericana de Seguridad en la Educación, 12(1), 102-118.

Guzmán, E., & Ortiz, V. (2022). Normativas de seguridad física en instituciones educativas:Avances y desafíos. Revista de Ciencias y Tecnologías Educativas, 24(3), 75-90.

L. ANEXOS

Figura 11: Caja de la fuente de alimentación.

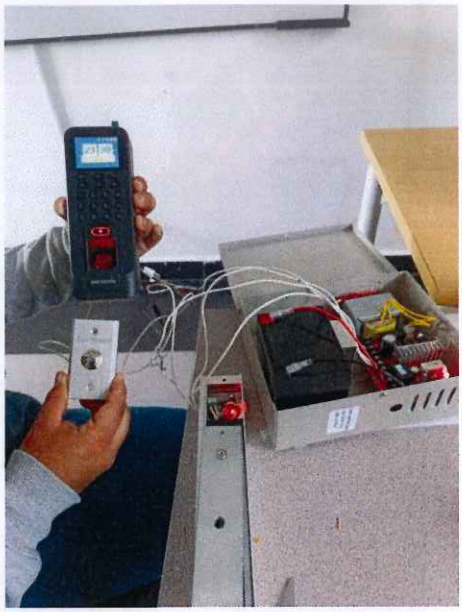


Descripción: Caja de la fuente de alimentación listo para el uso.

Figura 12: Rejas.

Descripción: Reja completa para las ventanas del laboratorio de cómputo.

Figura 13: Conexión del biométrico.



Descripción: Prueba de conexión del biométrico con la caja de fuente de alimentación.

Figura 14: Biométrico.

Descripción: Instalación del biométrico en el laboratorio de cómputo.

Figura 15: Placa de metal.

Descripción: Colocación de la placa de metal.

Figura 16: Cerradura electromagnética.

Descripción: Instalación de la puerta magnética.

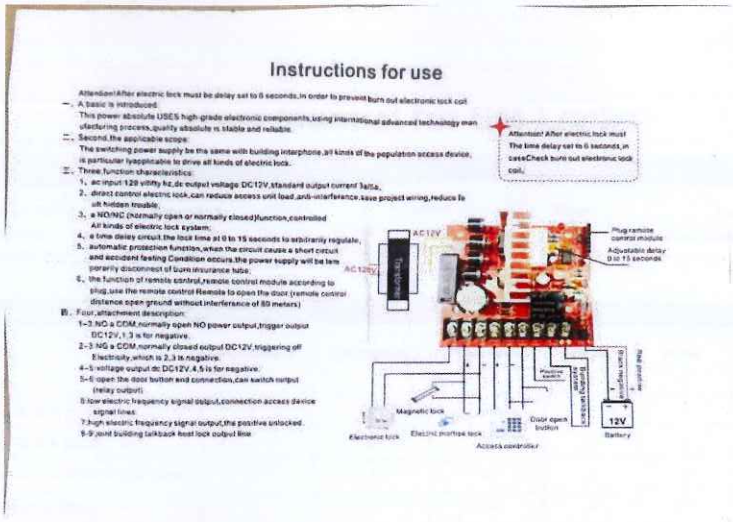
Figura 17: Botón de salida.

Descripción: Colocación del botón de salida.

Figura 18: Botón de salida y cerradura electromagnética.

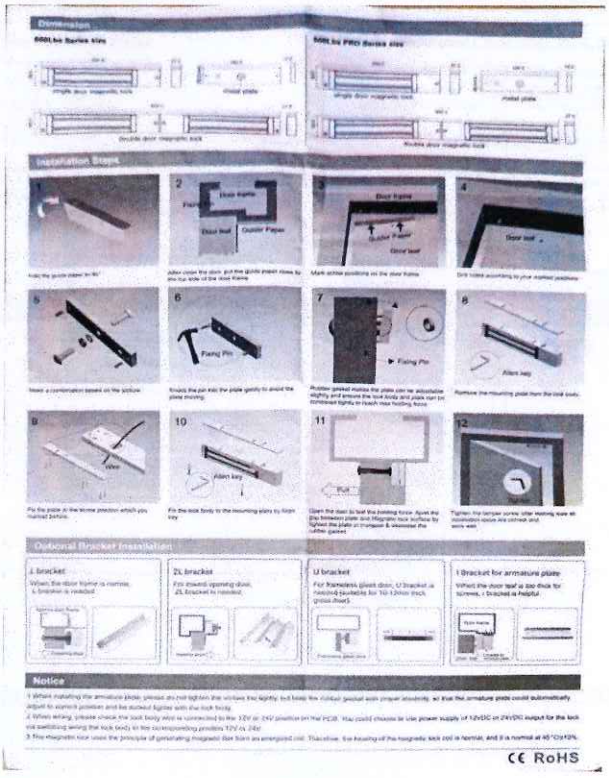
Descripción: Vista completa del botón y la cerradura magnética correctamente instalados.

Figura 19: Instrucción de uso.



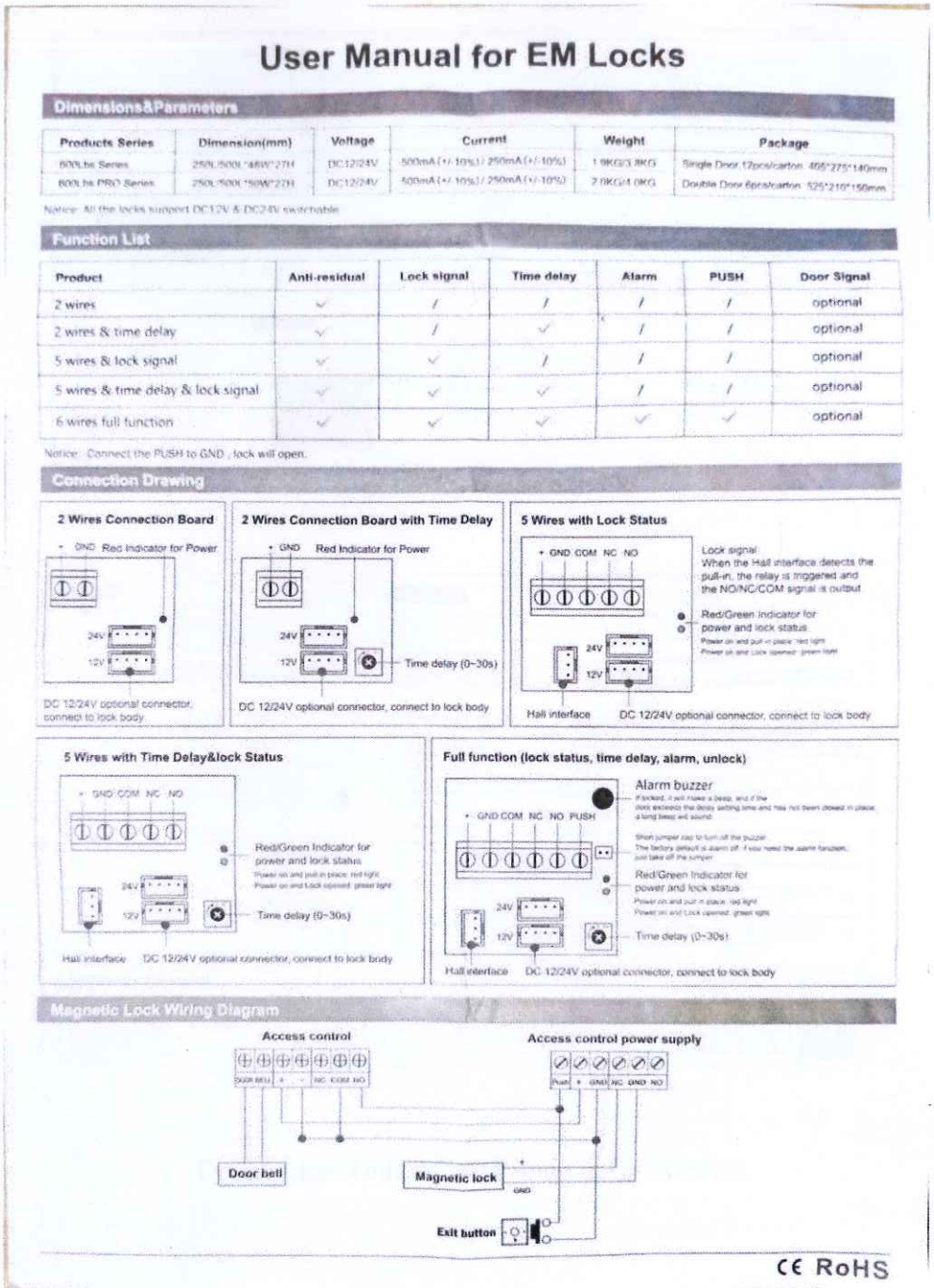
Descripción: Instrucciones para el uso de la conexión del biométrico y la puerta magnética ala fuente de alimentación.

Figura 20: Guía de instalación.



Descripción: Guía de instalación de la placa de metal y la cerradura electromagnética.

Figura 21: Manual de usuario.



User Manual for EM Locks

Dimensions&Parameters

Products Series	Dimension(mm)	Voltage	Current	Weight	Package
600Lbs Series	250L/500L*48W*27H	DC12/24V	500mA(+/-10%)/ 250mA(+/-10%)	1.0KG/1.8KG	Single Door 12pcs/carton: 495*275*140mm
800Lbs PRO Series	250L/500L*50W*27H	DC12/24V	500mA(+/-10%)/ 250mA(+/-10%)	2.0KG/4.0KG	Double Door 6pcs/carton: 525*210*150mm

Notice: All the locks support DC12V & DC24V switchable

Function List

Product	Anti-residual	Lock signal	Time delay	Alarm	PUSH	Door Signal
2 wires	√	/	/	/	/	optional
2 wires & time delay	√	/	√	/	/	optional
5 wires & lock signal	√	√	/	/	/	optional
5 wires & time delay & lock signal	√	√	√	/	/	optional
6 wires full function	√	√	√	√	√	optional

Notice: Connect the PUSH to GND , lock will open.

Connection Drawing

2 Wires Connection Board

- GND Red Indicator for Power
- 24V
- 12V

DC 12/24V optional connector, connect to lock body

2 Wires Connection Board with Time Delay

- GND Red Indicator for Power
- 24V
- 12V
- Time delay (0~30s)

DC 12/24V optional connector, connect to lock body

5 Wires with Lock Status

- GND COM NC NO
- 24V
- 12V

Lock signal
When the Hall interface detects the pull-in, the relay is triggered and the NO/NC/COM signal is output

Red/Green indicator for power and lock status

Hall interface DC 12/24V optional connector, connect to lock body

5 Wires with Time Delay&lock Status

- GND COM NC NO
- 24V
- 12V
- Time delay (0~30s)

Red/Green Indicator for power and lock status

Hall interface DC 12/24V optional connector, connect to lock body

Full function (lock status, time delay, alarm, unlock)

- GND COM NC NO PUSH
- 24V
- 12V
- Time delay (0~30s)

Alarm buzzer

Red/Green Indicator for power and lock status

Hall interface DC 12/24V optional connector, connect to lock body

Magnetic Lock Wiring Diagram

Access control

Access control power supply

Door bell

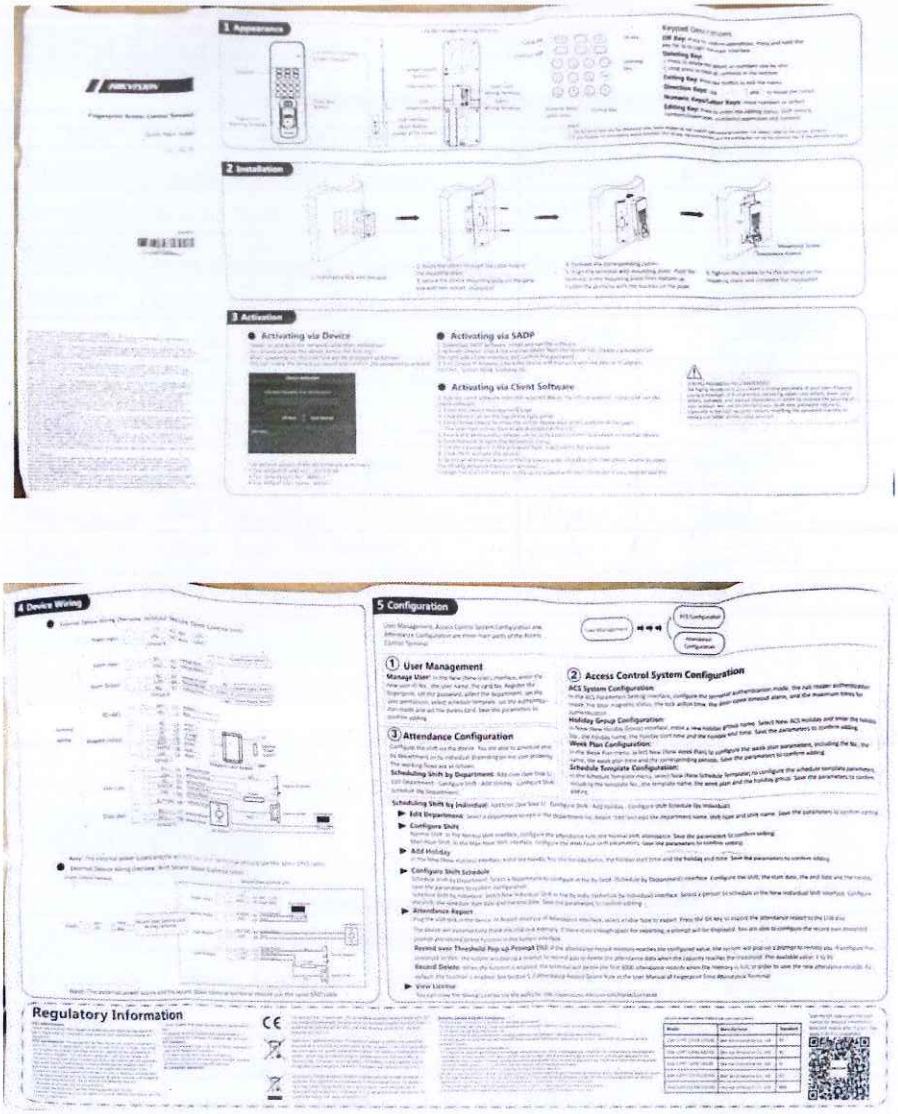
Magnetic lock

Exit button

CE RoHS

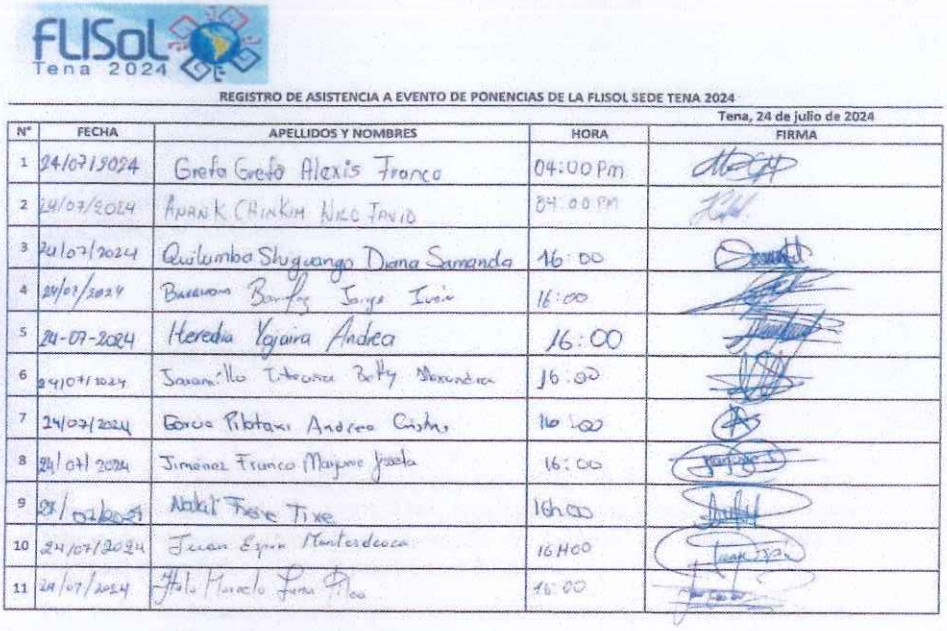
Descripción: Manual de usuario de cerradoras electromagnéticas.

Figura 22: Guía de instalación.



Descripción: Guía de instalación del biométrico.

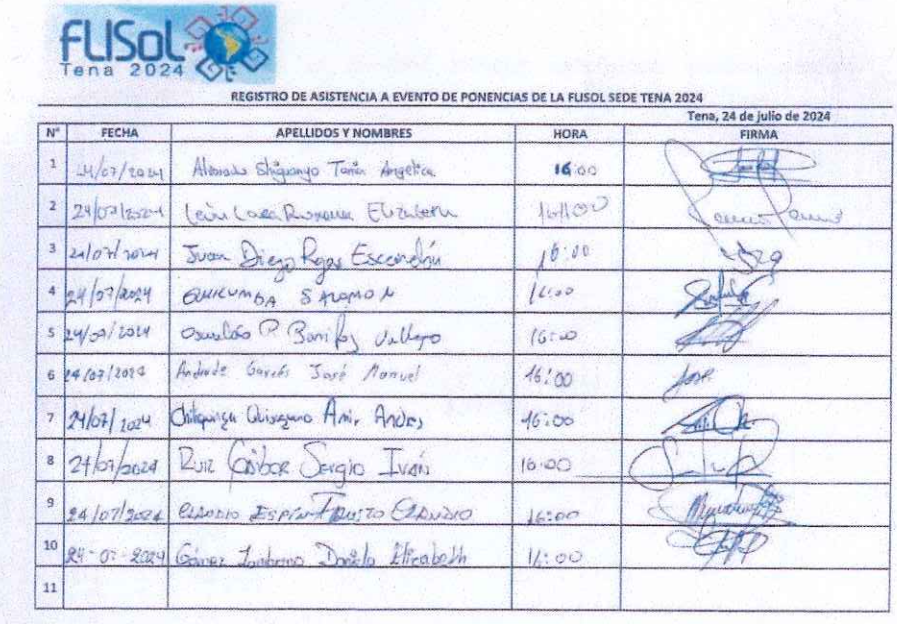
Figura 23: Capacitación



REGISTRO DE ASISTENCIA A EVENTO DE PONENCIAS DE LA FLISOL SEDE TENA 2024

Tena, 24 de julio de 2024

N°	FECHA	APELLIDOS Y NOMBRES	HORA	FIRMA
1	24/07/2024	Grefa Grefa Alexis Franco	04:00 Pm	
2	24/07/2024	APANK CHINKIM NILO JAVID	04:00 PM	
3	24/07/2024	Quilumba Shiguango Diana Samanda	16:00	
4	24/07/2024	Buenaños Benítez Jorge Iván	16:00	
5	24-07-2024	Heredia Yajaira Andrea	16:00	
6	24/07/2024	Jaramillo Titocaza Betty Alexandra	16:00	
7	24/07/2024	Gavo Pilataxi Andrea Cristina	16:00	
8	24/07/2024	Jimenez Franco Mayra Jacqueline	16:00	
9	24/07/2024	Nakai Tsere Tixe	16h00	
10	24/07/2024	Juan Espin Montesdeoca	16H00	
11	24/07/2024	Abel Marcelo Lema Tipan	16:00	



REGISTRO DE ASISTENCIA A EVENTO DE PONENCIAS DE LA FLISOL SEDE TENA 2024

Tena, 24 de julio de 2024

N°	FECHA	APELLIDOS Y NOMBRES	HORA	FIRMA
1	24/07/2024	Alvarado Shiguango Tania Angelica	16:00	
2	24/07/2024	León Lara Rosmeira Elizabeth	16h00	
3	24/07/2024	Juan Diego Rojas Escobar	16:00	
4	24/07/2024	QUILUMBA SALOMON	16:00	
5	24/07/2024	Osvaldo P Benitez Vallejo	16:00	
6	24/07/2024	Andrade Garcés José Manuel	16:00	
7	24/07/2024	Chiliquinga Quishpe Ana Anda	16:00	
8	24/07/2024	Ruiz Cabrera Sergio Iván	16:00	
9	24/07/2024	Rosero Espin Fausto Gerardo	16:00	
10	24-07-2024	Gómez Gutierrez Daniela Elizabeth	16:00	
11				

Descripción: Firma de asistencia a la capacitación sobre la seguridad física del laboratorio decómputo del Instituto Superior Tecnológico Tena.

Figura 24: Autorización de la implementación

Tena, 7 de agosto de 2024

Magister
Juan Diego Rojas
RECTOR ENCARGADO DEL ISTTENA
Presente,

De nuestra consideración:

Nosotros, Sr. Kay Zack Tapuy Tanguila con CC: 1550201808 y Sr. Jonathan Andrés Chavez Pindolema con CC: 1550174344, estudiantes de 5to sección nocturna de la carrera de Tecnología Superior en Desarrollo de Software, nos dirigimos ante su autoridad para saludar y desearle éxitos en sus funciones.

Por medio del presente ponemos en su conocimiento que estamos en el proceso de titulación con Tema de proyecto: *Implementar estrategias de seguridad física en el laboratorio de cómputo del Instituto Superior Tecnológico Tena*; por tal motivo solicitamos respetuosamente nos **AUTORICE** la colocación de protectores metálicos en las ventanas y control de acceso biométrico en el laboratorio de computación, esto con la finalidad de finalizar con éxito nuestro proyecto el mismo que beneficiará a la institución que nos acogió durante nuestra estancia académica.

Seguros de contar con su favorable atención, anticipamos nuestros sinceros agradecimientos.

Atentamente,

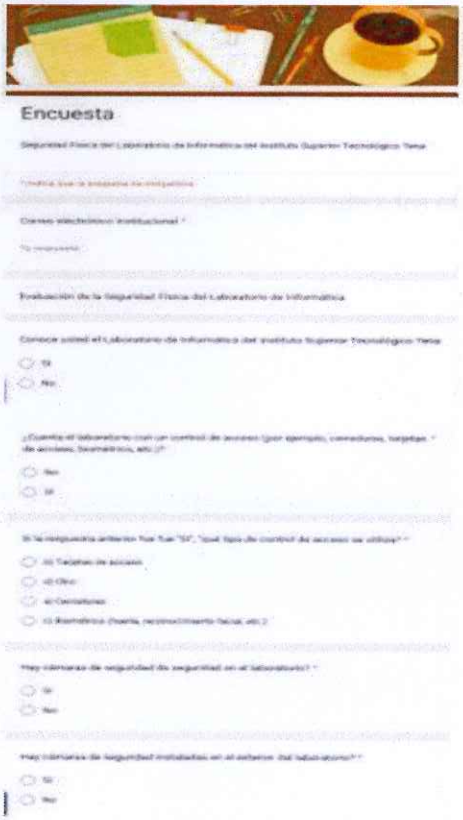
Sr. Kay Zack Tapuy Tanguila
CC: 1550201808
ESTUDIANTE

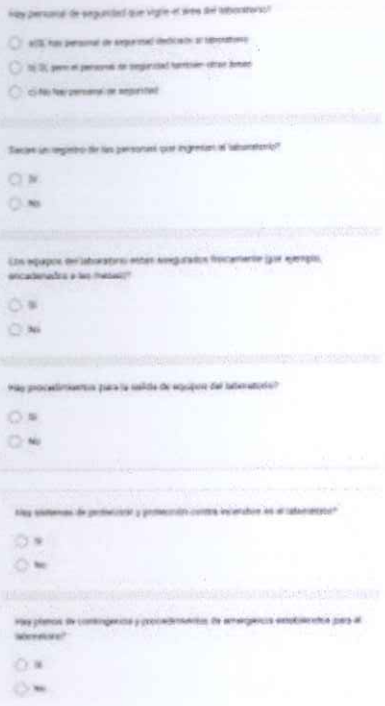
Sr. Jonathan Andrés Chávez Pindolema
CC: 1550174344
ESTUDIANTE

Figura 25: Implementación de las rejas al exterior del laboratorio de cómputo

Descripción: Colocación de rejas al exterior del laboratorio de cómputo

Figura 26: Encuesta





Descripción: Encuesta vacía realizada a los estudiantes.