REPÚBLICA DEL ECUADOR

CARRERA DE TECNOLOGÍA SUPERIOR EN
DESARROLLO DE SOFTWARE

CREACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN DEL INSTITUTOSUPERIOR TECNOLÓGICO TENA.

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

AUTORES: Deysi Denice Yumbo
ShiguangoLuz María
Alvarado Cerda
TUTOR: Ing. Darwin Fernando Núñez Collantes

Tena - Ecuador
2023-IIS

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, CREACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN DEL INSTITUTO SUPERIOR TECNOLÓGICO TENA, de autoría de las señoritas Deysi Denice Yumbo Shiguango, con CC. 1500947070, Luz María Alvarado Cerda con CC. 1501071375 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 exigen el respectivo reglamento e institución.

Tena, 05 de febrero de 2024

ING. FERNANDO NÚÑEZ C. MG.

TUTOR

CERTIFICACIÓN DEL TRIBUNAL CALIFICADOR

Tena, 5 de febrero de 2024

Los Miembros del Tribunal de Grado abajo firmantes, certificamos que el Trabajo de Integración Curricular denominado: CREACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN DEL INSTITUTO SUPERIOR TECNOLÓGICO TENA, presentado por Yumbo Shiguango Deysi Denice y Alvarado Cerda Luz María 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. Salomón Quilumba
PRESIDENTE DEL TRIBUNAL

Lcda. Marjorie Jiménez
MIEMBRO DEL TRIBUNAL

Ing. Oswaldo Bonifaz
MIEMBRO DEL TRIBUNAL

AUTORÍA

Nosotras, Deysi Denice Yumbo Shiguango, con CC: 1500947070, Luz María Alvarado Cerda, con CC: 1501071375 declaro ser autores del presente Trabajo de Integración Curricular denominado: CREACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN DEL INSTITUTO SUPERIOR TECNOLÓGICO 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.

AUTOR:

DEYSI DENICE YUMBO SHIGUANGO
CÉDULA: 1500947070

AUTOR:

LUZ MARÍA ALVARADO CERDA
CÉDULA: 1501071375

FECHA: Tena, 05 de febrero del 2024

CARTA DE AUTORIZACIÓN POR PARTE DEL AUTOR

Yo, Deysi Denice Yumbo Shiguango declaro ser autora del Trabajo de Integración Curricular titulado: CREACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN DEL INSTITUTO SUPERIOR TECNOLÓGICO TENA, como requisito para la obtención del Título de: TECNÓLOGO SUPERIOR EN DESARROLLO DE SOFTWARE: autorizo al Sistema Bibliotecario del Instituto Superior Tecnológico Tena, para que con fines académicos, muestre al 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 responsabiliza por el plagió o copia del presente trabajo que realice un tercero. Para constancia de esta autorización, en la ciudad de Tena, 05 de febrero de 2024, firma la autora.

AUTOR: Deysi Denice Yumbo Shiguango.
FIRMA:
CÉDULA: 1500947070
DIRECCIÓN: Archidona, Barrio San Bartolo
CORREO ELECTRÓNICO: deysi.yumbo@est.itstena.edu.ec
TELÉFONO: 0968992258

DATOS COMPLEMENTARIOS

TUTOR: Ing. Fernando Núñez.

TRIBUNAL DEL GRADO:

Ing. Salomón Quilumba. (Presidente).
Lcda. Marjorie Jiménez. (Miembro).
Ing. Oswaldo Bonifaz. (Miembro).

CARTA DE AUTORIZACIÓN POR PARTE DEL AUTOR

Yo, Luz María Alvarado Cerda, declaro ser autora del Trabajo de Integración Curricular titulado: CREACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN DEL INSTITUTO SUPERIOR TECNOLÓGICO TENA, como requisito para la obtención del Título de: TECNÓLOGO SUPERIOR EN DESARROLLO DE SOFTWARE: autorizo al Sistema Bibliotecario del Instituto Superior Tecnológico Tena, para que con fines académicos, muestre al 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 responsabiliza por el plagió o copia del presente trabajo que realice un tercero. Para constancia de esta autorización, en la ciudad de Tena, 05 de febrero de 2024, firma la autora.

AUTOR: Luz María Alvarado Cerda.
FIRMA:
CÉDULA: 1501071375
DIRECCIÓN: Av. Muyuna, Huayrayacu
CORREO ELECTRÓNICO: luz.alvarado@est.itstena.edu.ec
TELÉFONO: 0988845944

DATOS COMPLEMENTARIOS

TUTOR: Ing. Fernando Núñez.

TRIBUNAL DEL GRADO:

Ing. Salomón Quilumba. (Presidente).
Lcda. Marjorie Jiménez. (Miembro).
Ing. Oswaldo Bonifaz. (Miembro).

DEDICATORIA

Dedico este informe de TIC a Dios por haber permitido llegar hasta donde estoy, por ser el principal guía en mi camino y haberme ayudado a superar y vencer todos mis obstáculos.

A toda mi familia porque con sus oraciones, consejos y palabras de aliento hicieron de mí una mejor persona y de una u otra forma me acompañan en todos mis sueños y metas.

Autor: Luz Alvarado.

AGRADECIMIENTO

Quiero agradecer a las personas que forman parte de mi familia que me brindaron su apoyo incondicional para continuar y culminar con mis estudios.

Me agradezco a mí misma porque, me costó con tantas noches de desvelo, esfuerzo, sacrificio, para poder finalizar este trabajo.

Mi profundo agradecimiento al Instituto Superior Tecnológico Tena, a los profesores, quienes con la enseñanza de sus valiosos conocimientos hicieron que pueda crecer día a día como profesional, gracias a cada una de ustedes por su paciencia, dedicación, apoyo incondicional y amistad.

Autor: Deysi Yumbo

ÍNDICE

A. TEMA 1

B. RESUMEN 2

C. FUNDAMENTACIÓN DEL TEMA 4

3.1 Necesidad 4

3.2 Actualidad 4

3.3 Importancia 5

3.4 Presentación del problema profesional a responder 6

3.5 Delimitación 6

3.5.1 Delimitación Espacial 6

3.5.2 Delimitación Temporal 6

3.5.3 Delimitación Técnica 6

3.5.4 Unidades de Observación 7

3.6 Beneficiarios 7

3.6.1 Directos 7

3.6.2 Indirectos 7

4.1 Objetivo General 7

4.2 Objetivos Específicos 8

6.1 Temas y subtemas 9

6.1.1 Definición de un SGSI 11

6.1.2 El ciclo de mejora continua 11

6.1.3 Política 13

6.1.4 Inventario de activos 13

7.1 Materiales **16**

7.2 Equipos 17

7.3 Ubicación del Área de estudio 17

7.4 Tipo de investigación / estudio 17

7.5 Metodología para cada objetivo. 17

8 Bibliografía **29**

INDICE DE TABLAS

Tabla 1 *Asignaturas integradoras* 8
Tabla 2 *Ejemplo de inventario de activos* 14

INDICE DE FIGURAS

Figura 1 *Metodología PDCA* 12
Figura 2 *Pregunta 1* 20
Figura 3 *Pregunta 2* 20
Figura 4 *Pregunta 3* 21
Figura 5 *Pregunta 4* 22
Figura 6 *Pregunta 5* 22
Figura 7 *Pregunta 6* 23
Figura 8 *Pregunta 7* 23
Figura 9 *Pregunta 8* 24
Figura 10 *Verificación de control de acceso* 24
Figura 11 *Acceso al laboratorio de cómputo* 25
Figura 12 *Verificación de seguridad en el RACK* 25
Figura 13 *Acceso al rack área 3* 26
Figura 14 *Proyectores en aulas* 26
Figura 15 *Entrevista al personal de seguridad* 27

TEMA

CREACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN DEL INSTITUTO SUPERIOR TECNOLÓGICO TENA.

RESUMEN

La creación de políticas de seguridad informática para la Unidad de Tecnologías de la Información del Instituto Superior Tecnológico Tena es esencial con el fin de salvaguardar la integridad, confidencialidad y disponibilidad de la información.
Este proceso implica la revisión exhaustiva de la infraestructura tecnológica, la identificación de activos de información y la clasificación de datos sensibles. Se plantea la formulación de políticas y procedimientos específicos que aborden la gestión segura de la información, incluyendo aspectos como la recopilación, el almacenamiento y la transmisión de datos.

Se aplicó encuestas a los profesores con la finalidad de recopilar información indispensable para la elaboración del proyecto, el mismo que permitió tener una visión específica de la situación actual.
La implementación de mecanismos de seguridad tecnológica, junto con la capacitación del personal y auditorías internas de cumplimiento, se destacan como elementos clave en la estrategia. Este enfoque holístico busca no solo cumplir con las normativas legales, sino también fortalecer la cultura de seguridad informática en el Instituto Superior Tecnológico Tena, asegurando la protección efectiva de la información en un entorno tecnológico en constante evolución.

Palabras clave: Políticas, seguridad informática, TIC, ISO.

ABSTRACT

The creation of IT security policies for the Information Technology Unit of the Instituto Superior Tecnológico Tena is essential in order to safeguard the integrity, confidentiality and availability of information.

This process involves the exhaustive review of the technological infrastructure, the identification of information assets and the classification of sensitive data. The formulation of specific policies and procedures that address the secure management of information, including aspects such as data collection, storage and transmission, is proposed.

Surveys were applied to professors in order to gather indispensable information for the elaboration of the project, which allowed to have a specific vision of the current situation.

The implementation of technological security mechanisms, together with staff training and internal compliance audits, stand out as key elements in the strategy. This holistic approach seeks not only to comply with legal regulations, but also to strengthen the culture of information security in the Instituto Superior Tecnológico Tena, ensuring the effective protection of information in a constantly evolving technological environment.

Key words: Policies, information security, ICT, ISO.

Reviewed by:

BEd. Yefferson Intriago Burgos, M.Ed.
ID. 1313123976
Teacher of English Center of IST Tena.

A. FUNDAMENTACIÓN DEL TEMA

3.1 Necesidad

En el contexto actual, la información digital desempeña un papel fundamental en el funcionamiento de las instituciones educativas. El Instituto Superior Tecnológico Tena genera información diaria de docentes, estudiantes y directivos, la cual debe ser cuidada y protegida. Esta institución maneja plataformas de aprendizaje, plataformas de gestión académica y plataformas de información que podrían estar amenazadas o presentar algún tipo de vulnerabilidad.

La propagación de amenazas cibernéticas y la constante evolución de los entornos tecnológicos destacan la necesidad urgente de que el Instituto Superior Tecnológico Tena establezca políticas de seguridad informática alineadas a las necesidades actuales de la institución.

Específicamente, se requiere implementar políticas de administración, manejo y tratamiento de los datos, así como políticas de tratamiento de la información, con el fin de proteger los activos digitales y la privacidad de la comunidad educativa frente a posibles incidentes de seguridad.

Además, se busca crear una cultura organizacional de buenas prácticas en seguridad informática en el aspecto computacional y fortalezca la protección lógica de los activos informáticos de la institución.

3.2 Actualidad

El Instituto Superior Tecnológico Tena genera gran cantidad de información digital en sus plataformas virtuales, la cual debe ser protegida. Sin embargo, pese al uso de estas plataformas, no existen políticas que regulen el acceso a los diferentes perfiles de usuario.

Esta ausencia de directrices específicas en materia de seguridad informática dentro de la Unidad de TIC ha dejado a la institución vulnerable frente a posibles brechas de seguridad,

pérdida de datos sensibles y amenazas que podrían comprometer la integridad de los sistemas informáticos, así como la confidencialidad de la información.

Es relevante que el Instituto Superior Tecnológico Tena establezca políticas de seguridad informática para mitigar riesgos potenciales, garantizar la continuidad operativa y proteger efectivamente los activos de información de la institución. Dichas políticas deben regular el acceso a las plataformas virtuales según los diferentes perfiles de usuario, con el fin de salvaguardar los datos generados y evitar incidentes que puedan paralizar las operaciones o poner en riesgo la privacidad de estudiantes, docentes y personal administrativo.

3.3 Importancia

La tecnología en constante evolución presenta mejores servicios de acceso a la información en todo momento y desde cualquier punto con conexión a internet. Esto permite el tratamiento de información para el análisis y medición de la gestión educativa. Sin embargo, esto también hace necesario que el tratamiento de los procesos de información se rija por lineamientos claros de manejo y seguridad.

El presente proyecto busca proporcionar un marco sólido y adaptado a las circunstancias específicas del Instituto Superior Tecnológico Tena. Se pretende brindar un enfoque integral para la creación de políticas de seguridad informática que aseguren la protección y confidencialidad de la información, al tiempo que se promueve un entorno digital confiable y seguro para todas las actividades del Instituto.

Además, este proyecto contribuirá a la formación de una cultura de seguridad informática entre profesores, estudiantes y personal administrativo. Esto se logrará promoviendo prácticas seguras y una gestión eficiente de la información, acordes a los lineamientos establecidos.

De esta manera se podrán aprovechar los beneficios de las nuevas tecnologías para la educación, minimizando los riesgos asociados al manejo de información delicada en el ámbito de gestión educativa.

3.4 Presentación del problema profesional a responder

La Unidad de TIC del Instituto Superior Tecnológico Tena, carece de políticas de seguridad informática lo que ha ocasionado pérdida de información, negligencia de los usuarios entre otros.

Campo: Tecnologías de la Información y Comunicación
Área: Gestión de Seguridad Informática
Aspecto: Políticas de seguridad informática
Sector: Seguridad Informática
Línea de investigación: Tecnologías de la información y comunicación.

3.5 Delimitación

3.5.1 Delimitación Espacial

El Trabajo de Integración Curricular se lo realizará en el Instituto Superior Tecnológico Tena, el mismo que está ubicado en la vía Tena-Archidona en el km 1,5, provincia de Napo.

3.5.2 Delimitación Temporal

El proyecto se lo efectuará en el Periodo Académico 2023-IIS.

3.5.3 Delimitación Técnica

El presente proyecto consiste en realizar la Creación de Políticas de Seguridad Informática para Unidad de Tecnologías de la Información y Comunicación del Instituto Superior Tecnológico Tena las mismas que se argumentará según las directrices de la norma internacional ISO 27001 Seguridad de la información.

3.5.4 Unidades de Observación

Las unidades de observación que se contemplan para este trabajo están enfocadas directamente a la Unidad de TIC del Instituto Superior Tecnológico Tena. La accesibilidad a la información y las fuentes de datos es un criterio importante para seleccionar las unidades de observación. Al enfocarnos en la Unidad de TIC del Instituto Tecnológico Tena se facilita la recolección de datos relevantes a través de entrevistas, observación directa y acceso a documentación interna. Centrarnos en esta unidad permitirá obtener información valiosa y representativa sobre la gestión de TIC en instituciones de educación superior tecnológica.

3.6 Beneficiarios

3.6.1 Directos

- Instituto Superior Tecnológico Tena.

3.6.2 Indirectos

- Profesores
- Estudiantes
- Personal administrativo.

B. OBJETIVOS

4.1 Objetivo General

- Crear Políticas de Seguridad Informática para Unidad de Tecnologías de la Información del Instituto Superior Tecnológico Tena.

4.2 Objetivos Específicos

- Analizar la situación actual del IST Tena en referencia a la Seguridad Informática para el planteamiento de mejoras en el tratamiento de infraestructura e información.
- Plantear políticas de mejora para protección de datos que genera la infraestructura tecnológica del Instituto Superior Tecnológico Tena.
- Presentar un documento de uso y aplicación implementar políticas seguridad informática en base a las necesidades e infraestructura del Instituto Superior Tecnológico Tena

C. ASIGNATURAS INTEGRADORAS

Tabla 1
Asignaturas integradoras

ASIGNATURAS INTEGRADORAS	
Asignaturas	**Resultados de Aprendizaje**
Legislación Informática	Esta asignatura aborda las implicaciones éticas y legales de la seguridad informática, lo que es importante para garantizar el cumplimiento de las regulaciones y normativas.
Análisis de sistema	Es una parte esencial de la seguridad informática, ya que ayuda a comprender, evaluar y fortalecer la seguridad de los sistemas de información y comunicación en una organización.
Lenguaje y Comunicación	Las políticas de seguridad informática suelen incluir directrices y procedimientos para la comunicación entre los empleados, la gerencia y otros actores claves.

D. FUNDAMENTACIÓN TEÓRICA

6.1 Temas y subtemas

6.1.1 Glosario Términos Básicos relacionados a la Norma ISO27001

"Acceso.

- Cualquier acción realizada por un usuario en un sistema de información.

Amenaza.

- Evento que puede explotar una vulnerabilidad en un sistema de información y causar un daño.

Autenticación y Control de Acceso.

- Medidas de seguridad para asegurar que solo los usuarios autorizados tengan acceso a la información y los sistemas de la organización.

Autorización.

- Proceso por el cual se otorga permiso a un usuario para acceder a un recurso o realizar una acción.

Capacitación y Conciencia.

- Proceso para capacitar a los empleados sobre las políticas y procedimientos de seguridad de la información y para aumentar su conciencia sobre la importancia de la seguridad de la información.

Control de acceso.

- Procedimientos para garantizar que solo los usuarios autorizados puedan acceder a la información.

Control de acceso lógico.

- Medidas de seguridad para controlar el acceso a los sistemas y la información de la organización a través de controles de acceso basados en roles, contraseñas, autenticación multifactorial, entre otros.

Control de acceso físico.

- Medidas de seguridad para controlar el acceso a los edificios y las áreas físicas de la organización mediante controles de acceso físico como tarjetas de acceso, cámaras de seguridad, entre otros.

Política de Seguridad de la Información (Psi).

-Documento que establece los objetivos y principios de seguridad de la información de la organización.

Seguridad de la información.

- Medidas de seguridad para proteger la información de la organización, incluyendo su confidencialidad, integridad y disponibilidad.

Seguridad física.

- Medidas de seguridad para proteger los activos físicos de la organización.

Seguridad lógica.

- Medidas de seguridad para proteger los activos lógicos de la organización, como la información almacenada en sistemas informáticos.

6.1.2 Definición de un SGSI

Un Sistema de Gestión de la Seguridad de la Información (SGSI) es un conjunto de procesos que permiten establecer, implementar, mantener y mejorar de manera continua la seguridad de la información, tomando como base para ello los riesgos a los que se enfrenta la organización.

6.1.3 El ciclo de mejora continua

El ciclo PDCA está implícito en la propia estructura de la norma, por lo que a continuación se desarrolla este modelo de mejora continua que creemos que es necesario conocer. El modelo PDCA o "Planificar-Hacer-Verificar-Actuar" (Plan-Do-Check-Act, de sus siglas en inglés), consta de un conjunto de fases que permiten establecer un modelo comparable a lo largo del tiempo, de manera que se pueda medir el grado de mejora alcanzado.

- Plan:
  En esta fase se planifica la implantación del SGSI. Se determina el concepto texto de la organización, se definen los objetivos y las políticas que permitirán alcanzarlos. Se correspondería con los capítulos 4, 5, 6 y 7 de la Norma ISO/IEC 27001:2017.

- Do:
  En esta fase se implementa y pone en funcionamiento el SGSI. Se práctica las políticas y los controles que, de acuerdo al análisis de riesgo se han seleccionado para cumplirlas. Para ello debe de disponerse de procedimientos en los que se identifique claramente quién debe hacer qué

tareas, asegurando la capacitación necesaria para ello. Se correspondería con el capítulo 8 de la Norma ISO/IEC 27001:2017.

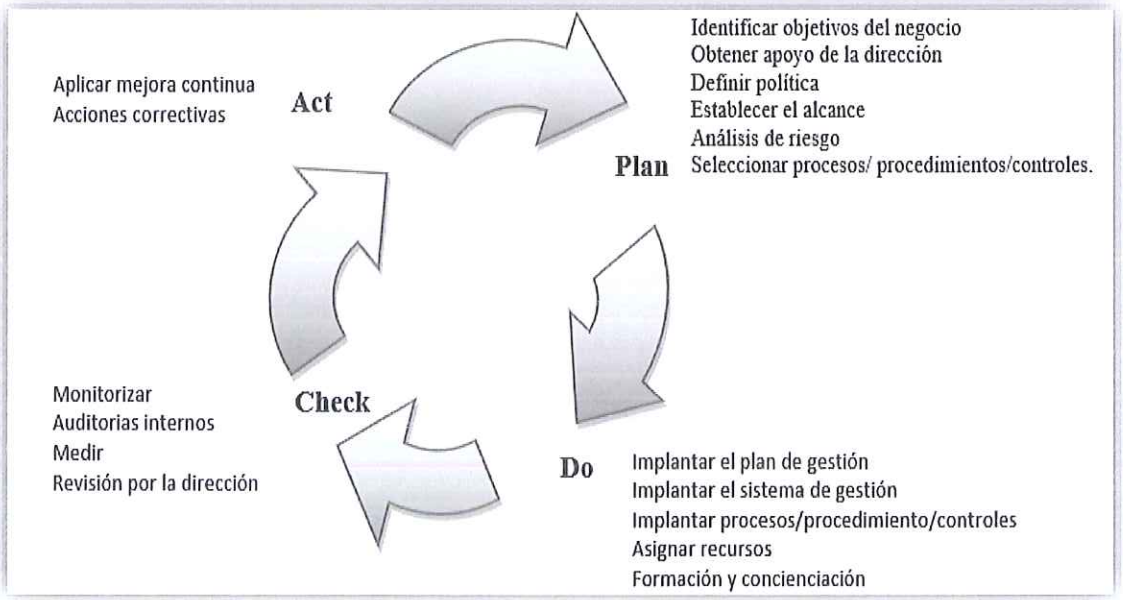
- Check:

  En esta fase se realiza la monitorización y revisión del SGSI. Se controla que los procesos se ejecutan de la manera prevista y que además permiten alcanzar los objetivos de la manera más eficiente. Se correspondería con el capítulo 9 de la Norma ISO/IEC 27001:2017.

- Act:

  En esta fase se mantiene y mejora el SGSI, definiendo y ejecutando las acciones correctivas necesarias para rectificar los fallos detectados en la anterior fase. Se correspondería con el capítulo 10 de la Norma ISO/TEC 27001:2017.

Figura 1
Metodología PDCA



Fuente: (Gomez & Pedro, 2018)

6.1.4 Política

Es la información documentada en la que se reflejan, en términos generales, los objetivos de la organización en materia de seguridad de la información y las principales líneas de acción que permitan proteger su información frente a las pérdidas de confidencialidad, integridad y disponibilidad. Tendrá en cuenta los requisitos del negocio, así como los contractuales, legales y estatutarios, los cuales quedarán reflejados en la misma.

En la política de seguridad de la información, la organización adquiere el compromiso de implantar y mejorar de manera continua el sistema de gestión.

6.1.5 Inventario de activos

Aunque la norma no exige la identificación de los activos para la realización de la evaluación de riesgo, sigue siendo una metodología válida y recomendable que da cumplimiento a los requisitos de la norma, y es coherente con el objetivo de un SGSI y la implantación de controles.

Tabla 2
Ejemplo de inventario de activos.

Nombre	*Descripción*	*Categoría*	*Ubicación*
Aplicaciones comerciales	Office, sistemas operativos, etc.	Aplicaciones	Servidor
Aplicación web RTT Ibérica	Página web de las empresas a través de la que se ofrecen servicios de alquiler y venta a los clientes	Aplicaciones	Servidor
Base de datos web	Base de datos donde se recogen los datos de los clientes.	Datos	Servidor
Sistema de correo electrónico	Utilizado para el envío de e-mails y catálogos a los clientes con las nuevas adquisiciones	Servicio	Servidor

Fuente: (Gomez & Pedro, 2018).

Normas Orientadas a la Seguridad de Información.

Norma ISO 27000: Es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. La Gestión de la Seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002.

Norma ISO/IEC 27000: Ofrece información general de las normas que componen la serie ISO 27000 aclarando sus alcances y dando la visión de conjunto de estas normas; cuenta con el vocabulario técnico usado en las normas, igualmente contiene una introducción al Sistema Integrado de Seguridad de la Información (SGSI).

Norma ISO/IEC 27001: Se considera la norma principal de la serie ISO 27000, donde se plasman los requisitos normativos para establecer el SGSI y su subsecuente operación y mejora; el SGSI girará alrededor de los riesgos y su tratamiento.

Norma ISO/IEC 27002: Establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Esto también incluye la selección, implementación y administración de controles, teniendo en cuenta los entornos de riesgo encontrados en la empresa."

Fuente: (Gomez & Pedro, 2018)

5.2 Marco Legal

"Leyes Nacionales

- Constitución de la República del Ecuador
  - ✓ Art. 18 - numeral 2: Reconoce y garantiza la libertad de expresión.
  - ✓ Art. 227: Establece la independencia de la Función Judicial.
  - ✓ Art. 229: Define la función de la Corte Constitucional.
  - ✓ Art. 234: Regula la creación y funcionamiento de la Contraloría General del Estado.
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
  - ✓ Art. 9: Establece la validez legal de las firmas electrónicas.
  - ✓ Art. 44: Regula la responsabilidad de los prestadores de servicios de certificación.
- Ley del Sistema Nacional de Registro de Datos Públicos.
  - ✓ Art. 1: Define el objeto y ámbito de aplicación de la ley.
  - ✓ Art. 26: Establece la gratuidad de la inscripción de actos y contratos en el registro.
- Ley Orgánica y Normas de Control de la Contraloría General del Estado.
  - ✓ Art. 3: Determina las competencias de la Contraloría General del Estado.
  - ✓ Art. 6: Regula la fiscalización y control de recursos públicos.
- Ley orgánica de transparencia y acceso a la información Publica

- ✓ Art. 5: Información Pública
- ✓ Art. 7: Difusión de la Información Pública

- Ley Orgánica del Servicio Público

✓ Art 4: Define los principios del servicio público.

✓ Art 43: Establece las condiciones para el ejercicio del derecho a la huelga de los servidores públicos.

Según el ACUERDO No. 004-CG-2023 en el cual se estipula las Normas de Control Interno para las entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos en el numeral 410-05.- Políticas y procedimientos menciona que "..La unidad de tecnologías de la información y comunicaciones definirá, documentará y difundirá las políticas, estándares y procedimientos que regulen las actividades relacionadas con la tecnología de información y comunicaciones en la organización, estos se actualizarán permanentemente e incluirán las tareas, los responsables de su ejecución, los procesos de excepción, el enfoque de cumplimiento y el control de los procesos que están normando, y comunicará al área de talento humano de la entidad para que aplique con oportunidad las sanciones administrativas a que hubiere lugar si no se cumplieran" ".

Fuente: (Estado, 2018, pág. Contraloría General del Estado. (2014).)

E. METODOLOGÍA

El siguiente capítulo se define de cómo se desarrolló el tema del proyecto Creación de Políticas de Seguridad Informática para Unidad de Tecnologías de la Información y del Instituto Superior Tecnológico Tena.

7.1 Materiales

- Libros físicos
- Libros electrónicos Leyes, normativas
- Internet

7.2 Equipos

- 1 computadora de escritorio (Hp, Dell)
- 1 impresora

7.3 Ubicación del Área de estudio

La ubicación área de estudio es en el km 1.5 en la vía Tena-Archidona, cantón Tena provincia de Napo en las Instalaciones del Instituto Superior Tecnológico Tena.

7.4 Tipo de investigación / estudio

La investigación de campo es un tipo de investigación que se realiza directamente en el entorno en el que ocurren los fenómenos estudiados, la investigación de campo implica la recopilación de información de primera mano mediante la observación directa, entrevistas, encuestas u otras técnicas de recolección de datos en el lugar de interés. En este sentido se efectuó encuestas a los profesores del Instituto Superior Tecnológico Tena con la finalidad de conocer la situación actual en lo que corresponde a políticas de seguridad informática en el IST Tena.

7.5 Metodología para cada objetivo.

Objetivo Específico 1:

Analizar la situación actual del IST Tena en referencia a la Seguridad Informática para el planteamiento de mejoras en el tratamiento de infraestructura e información.

Evaluación de la Infraestructura Tecnológica:

Se efectuó una visita en la cual se realizó la observación detallada de la infraestructura tecnológica del IST Tena, identificando activos críticos, sistemas de red, servidores y dispositivos de almacenamiento los mismo que no cuentan con medidas de seguridad física.

Revisión de Políticas de Seguridad:

Se realizó el análisis de las Normas de uso para el correo electrónico institucional del IST Tena, Normas de seguridad del laboratorio de computación del Instituto Superior Tecnológico Tena, las mismas que son políticas y procedimientos actuales relacionados con la seguridad informática en el IST Tena para evaluar su efectividad y su alineación con las mejores prácticas de seguridad.

Entrevistas y Encuestas:

Se efectuó encuestas a los profesores y entrevista al responsable de la unidad de TIC del IST Tena para comprender las percepciones sobre la seguridad informática y obtener información sobre incidentes pasados o potenciales riesgos.

Análisis de Incidentes Anteriores:

Se procedió a entrevistar al responsable de la unidad de TIC del IST Tena con la finalidad de conocer sobre los incidentes de seguridad anteriores, identificando las causas subyacentes, las lecciones aprendidas y las áreas que requieren mejoras inmediatas.

Evaluación del Cumplimiento Normativo:

Se verifica por medio del responsable de la unidad de Tecnologías de información y comunicación del IST Tena el cumplimiento de las normativas y regulaciones existentes en materia de seguridad informática que apliquen al IST Tena, identificando posibles áreas de no conformidad.

Capacitación y Concientización:

Se verificó mediante entrevista con el responsable de la unidad de TIC que no existe un Plan de capacitación y concientización sobre seguridad informática para los profesores y personal administrativo del instituto, esto permitirá mejorar la cultura de seguridad y reducir posibles riesgos causados por desconocimiento.

Revisión de Controles de Acceso y Autenticación:

Se realizó una visita a las instalaciones físicas para realizar una observación detallada de la seguridad física y control de acceso con la finalidad de evaluar los controles de acceso físicos y lógicos, así como los métodos de autenticación utilizados en el IST Tena, para asegurar la protección adecuada de los recursos tecnológicos.

Objetivo Específico 2:

Plantear políticas de mejora para protección de datos que genera la infraestructura tecnológica del Instituto Superior Tecnológico Tena.

Según las encuestas aplicadas a los profesores del instituto, se plantea políticas de seguridad informática, la misma que pretende regular aspectos en los que hasta el momento existe falencias por el desconocimiento de los usuarios.

Objetivo Específico 3:

Presentar un documento de uso y aplicación de políticas seguridad informática en base a las necesidades e infraestructura del Instituto Superior Tecnológico Tena.

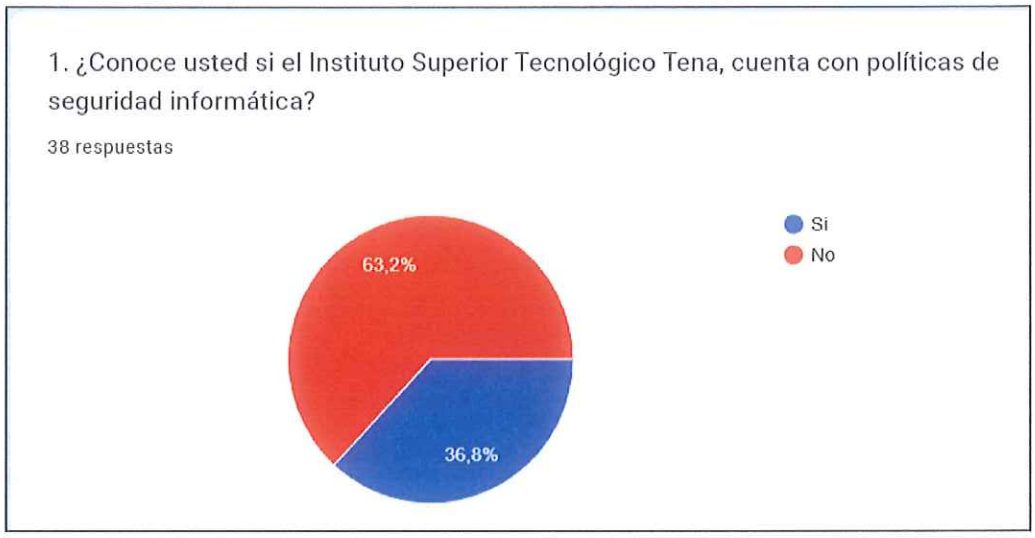
Se elabora un documento adicional donde constan las políticas de seguridad informática que el Instituto Superior Tecnológico Tena puede acoger por medio de la unidad de Tics.

F. RESULTADOS

Para realizar el Análisis de la situación actual del IST Tena en referencia a la Seguridad Informática para el planteamiento de mejoras en el tratamiento de infraestructura e información se procedió a efectuar encuesta a los profesores y entrevista personalizada al responsable de la unidad de tecnologías de la información y comunicación del instituto.

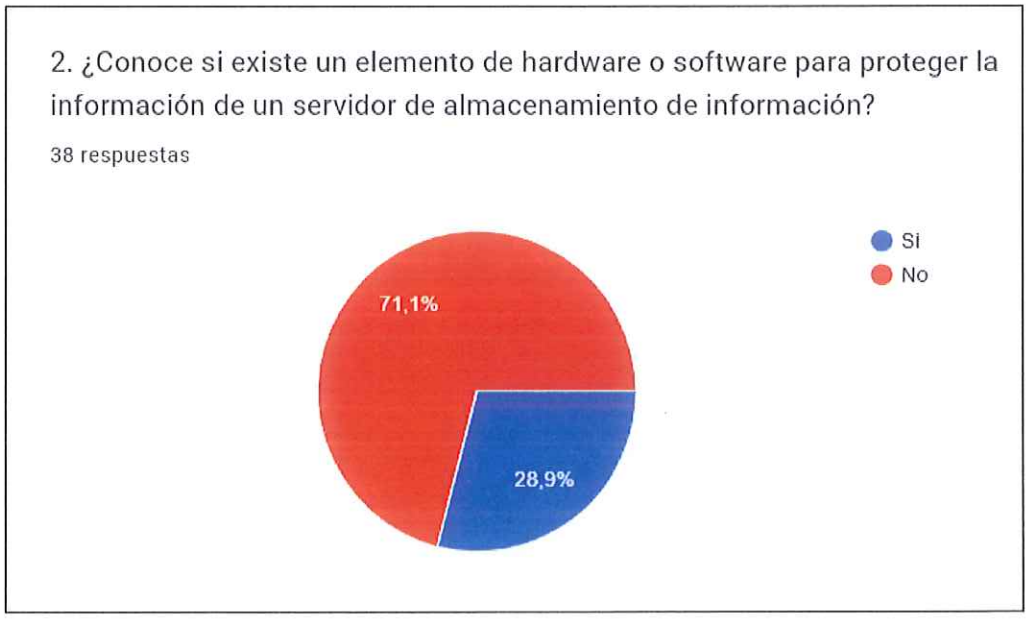
Interpretación de la encuesta realizada a los profesores del IST Tena.

Figura 2
Pregunta 1



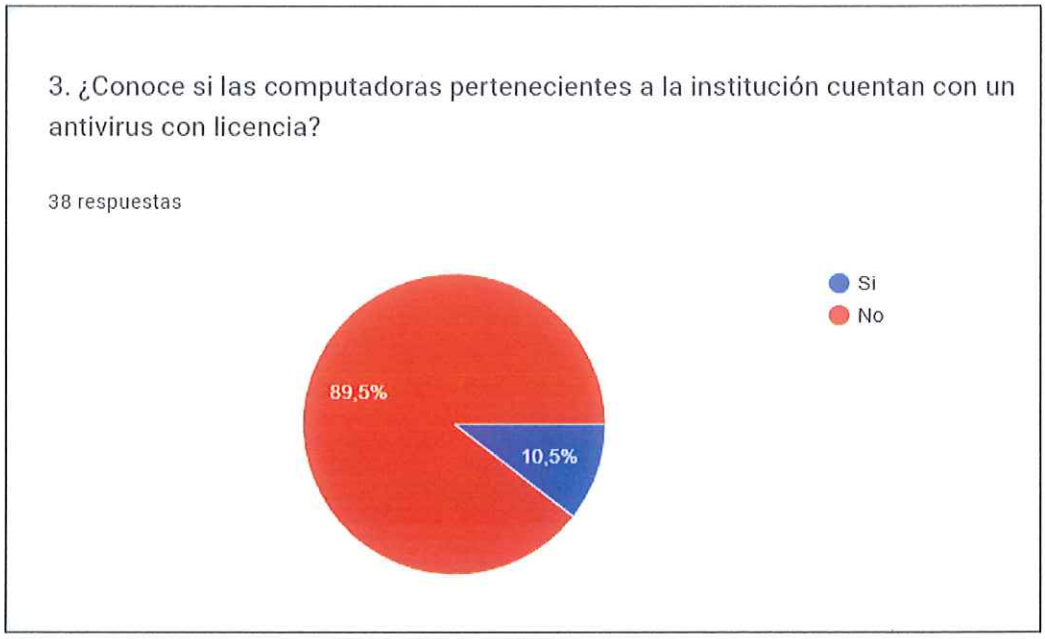
Interpretación: del 100% el 63.2% desconoce si el IST Tena, cuenta con políticas de seguridad informática, mientras que el 36.8% manifiesta que SI conoce que el IST Tena dispone de políticas de seguridad informática.

Figura 3
Pregunta 2



Interpretación: el 71,1% menciona que desconoce de la existencia de hardware o software para proteger la información de un servidor de almacenamiento, mientras que el 28.9% menciona lo contrario.

Figura 4
Pregunta 3

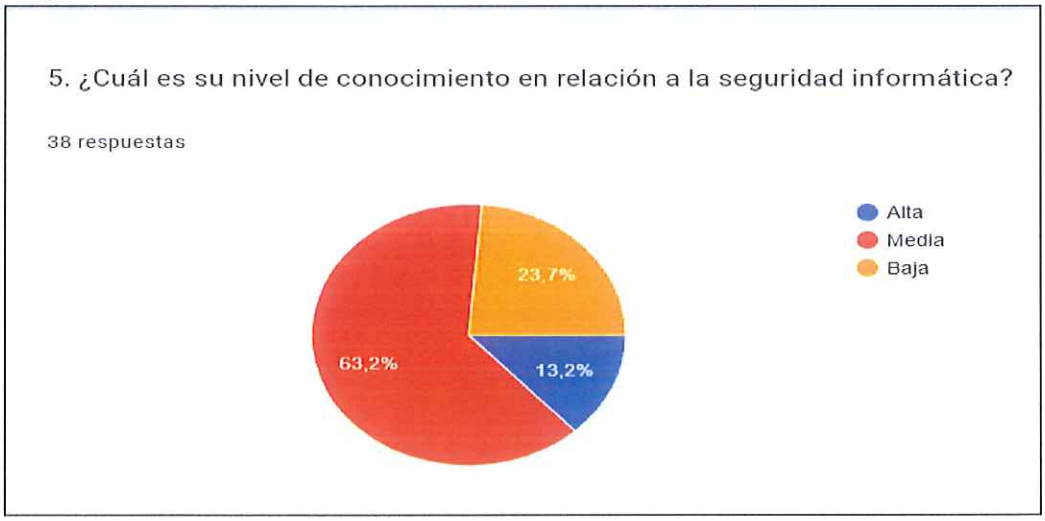


Interpretación: el 89.5% de encuestados manifiestan desconocer que las computadoras pertenecientes a la institución tengan antivirus con licencia, mientras que el 10.5% revelan lo contrario.

Figura 5
Pregunta 4

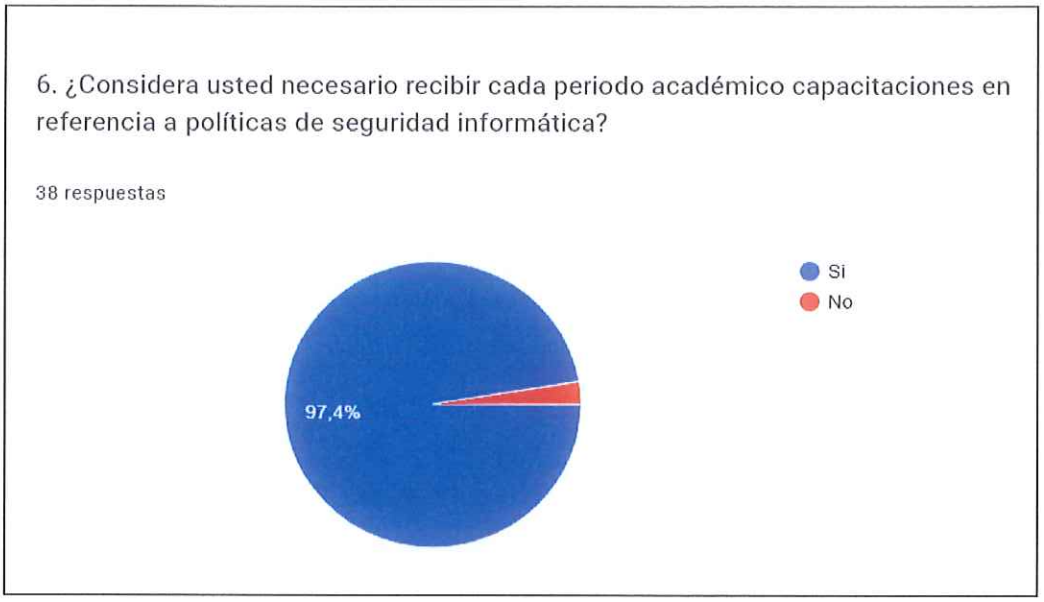
Interpretación: el 60.5% manifiesta que muy alto la importancia de contar con estándares de seguridad informática, mientas que el 21.1% considera alta y el 15.8% media.

Figura 6
Pregunta 5



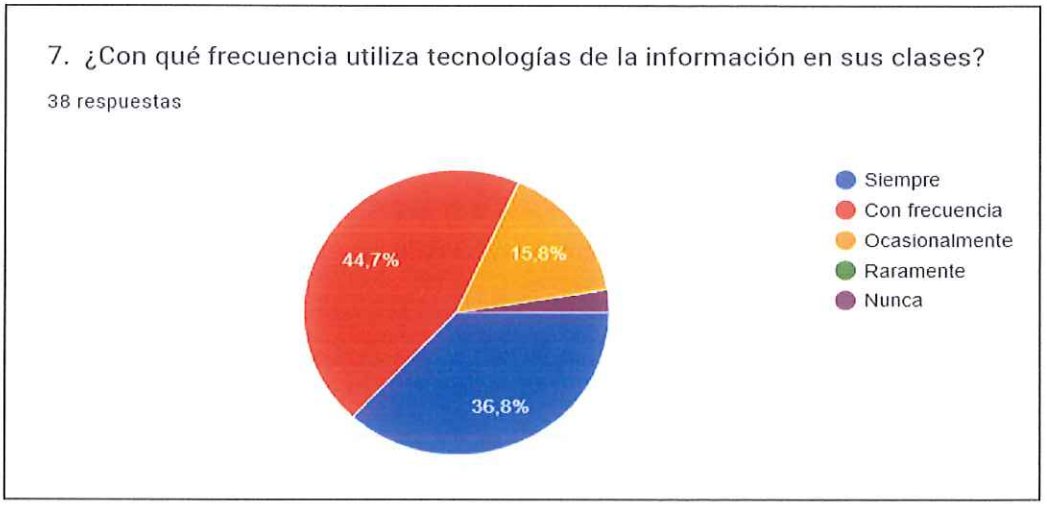
Interpretación: el 63.2% de los encuestados manifiesta que el nivel de conocimiento en relación a la seguridad informática es medio, mientas que el 23.7% dice ser baja y el 13.3% menciona que es alta.

Figura 7
Pregunta 6



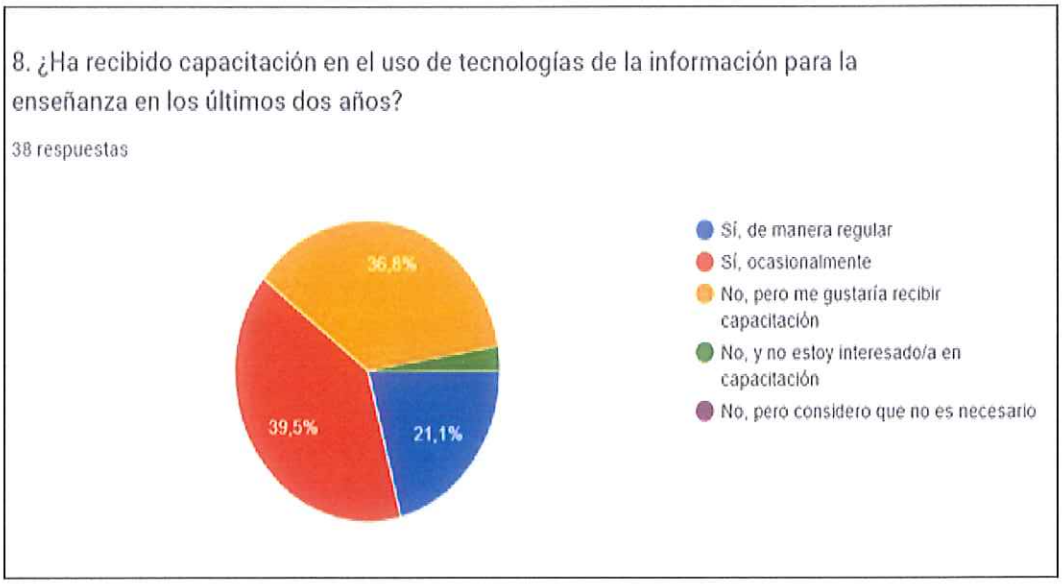
Interpretación: en base a la pregunta. Considera usted necesario recibir cada periodo académico capacitaciones en referencia a políticas de seguridad informática el 97.4% de encuestados manifiesta SI.

Figura 8
Pregunta 7



Interpretación: el 44.7% manifiesta que con frecuencia utiliza tecnologías de la información en sus clases, mientras que el 36.8% indica que Siempre y el 15.8% ocasionalmente.

Figura 9
Pregunta 8



Interpretación: el 39.5% manifiesta que Sí, ocasionalmente en relación que ha recibido capacitación en el uso de tecnologías de la información para la enseñanza en los últimos dos años, mientas que el 36.8% menciona no, pero me gustaría recibir capacitación y 21.1% indica sí, de manera regular.

Visita realizada con la finalidad de observar las instalaciones

Figura 10
Verificación de control de acceso

Nota. como parte de seguridad física se verificó que el acceso al cuarto de servidores del IST Tena es por medio de un biométrico.

Figura 11

Acceso al laboratorio de cómputo

Nota. el laboratorio de cómputo cuenta con puerta de estructura metálica como mecanismo de seguridad física.

Figura 12

Verificación de seguridad en el RACK

Nota. se verifica que el rack ubicado en el laboratorio cuenta con seguridad.

Figura 13

Acceso al rack área 3

Nota. se verifica el control de acceso al rack que interconecta al área 3.

Figura 14

Proyectores en aulas

Nota. se verificó y constató que los proyectores que están colocados en las aulas cuentan con protección y seguridad física.

Figura 15

Entrevista al personal de seguridad

Nota. se realizó una entrevista con la finalidad de conocer ciertos aspectos relacionados con la seguridad física con las que cuenta el instituto.

G. CONCLUSIONES

- Se analizó la situación actual del IST Tena en referencia a la Seguridad Informática para el planteamiento de mejoras en el tratamiento de infraestructura e información.
- Se elaboró las políticas de mejora para protección de datos que se genera dentro de la infraestructura tecnológica del Instituto Superior Tecnológico Tena.
- Se genero un consolidado de las políticas seguridad informática en base a las necesidades e infraestructura del Instituto Superior Tecnológico Tena

H. RECOMENDACIONES

- Revisar constantemente las políticas con la finalidad de actualizar según las necesidades institucionales, pese a que sean planteado las políticas es necesario seguir implementando otras sub-políticas con el fin de mantener en actualidad la protección de la información.
- Planificar capacitaciones dirigidas a los profesores en el área de Tecnologías de la información y seguridad informática con la finalidad de generar cultura en seguridad informática.
- Socializar las políticas de seguridad informática con el personal que labora en el Instituto Superior Tecnológico Tena.

I. BIBLIOGRAFÍA

8 Bibliografía

Gomez, L., & Pedro, F. (2018). *Cómo implantar un SGSI según ISO/IEC 27001 y su aplicacion de Esquema Nacional de Seguridad.* Colombia: AENOR INTERNACIONAL, S.A.U.

Hacker Mentor. (s.f.). Glosario de Términos ISO 27001. Hacker Mentor. https://www.hacker-mentor.com/glosarioterminosiso27001

Glosario básico ciberseguridad y hacking ético. (s/f). Hacker-mentor.com. Recuperado el 21 de enero de 2024, de https://www.hacker-mentor.com/glosariociberseguridad

Contraloría General del Estado. (2014). Manual de auditoría de gestión [Archivo PDF]. Recuperado de https://www.contraloria.gob.ec/WFDescarga.aspx?id=1486&tipo=mul

J. ANEXOS

Anexo 1.- Oficio de autorización para ejecutar encuesta

REPÚBLICA DEL ECUADOR

INSTITUTO SUPERIOR TECNOLÓGICO TENA
Tecnología, Innovación y Desarrollo

Secretaría de Educación Superior, Ciencia, Tecnología e Innovación

Oficio N° ISTT-R-2023-783-OF
Tena, 13 de diciembre de 2023

Señorita
Deysi Yumbo
ESTUDIANTE DEL IST TENA

Señorita
Luz Alvarado
ESTUDIANTES DEL IST TENA
Presente

De mi consideración:

Con un cordial saludo y en atención a su documento s/n de fecha 11 de diciembre de 2023, que en su parte pertinente manifiesta: *(...) solicitamos nos **AUTORICE** la ejecución de encuestas a los profesores, personal administrativo y personal de la Unidad de TIC, con la finalidad de recopilar información relevante para la elaboración de nuestro Trabajo de Integración Curricular titulado: **Creación de políticas de seguridad Informática para la Unidad de Tecnologías de la Información del Instituto Superior Tecnológico Tena** (...)*

Por lo expuesto, comunico que se autoriza realizar la actividad en mención; para lo cual deberá coordinar con la Unidad de Comunicación.

A la Coordinación de la Carrera de Tecnología Superior en Desarrollo de Software, brindar todas las facilidades.

Con sentimiento de consideración y estima.

Atentamente,

LORENA PILAR YÁNEZ PALACIOS

Ing. Lorena Pilar Yánez Palacios., MEd.
RECTORA DEL INSTITUTO SUPERIOR TECNOLÓGICO TENA

c.c.: *Mgs. Diego Rojas, VICERRECTOR*
Ing. Patricio Bonifaz, COORDINADOR DE CARRERA
Lcda. Verónica Zuña, RESPONABLE DE LA UNIDAD DE COMUNICACIÓN

Anexo 2.- *Verificación de seguridad en el RACK que se encuentra ubicado en el laboratorio.*

Anexo 3.- *Verificación de seguridad en el RACK que interconecta el área 3.*