UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TECNOLOGÍA DE LA INFORMACIÓN
EXAMEN COMPLEXIVO

Componente Práctico, previo a la obtención del Título de:

INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

"IMPLEMENTACIÓN DE UN PLAN DE ACCIÓN PARA LAS BUENAS PRÁCTICAS EN LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DEL DEPARTAMENTO DE TIC´S DE LA UPSE"

AUTOR

PANIMBOZA PANCHANA ANTHONY MAURICIO

TUTOR

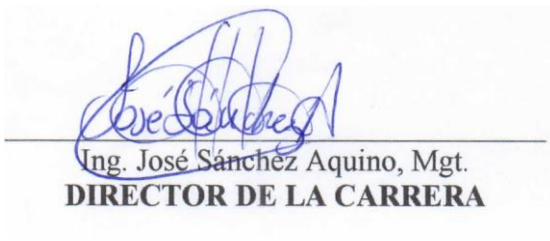
ING. IVÁN CORONEL SUÁREZ, MSIA

LA LIBERTAD- ECUADOR

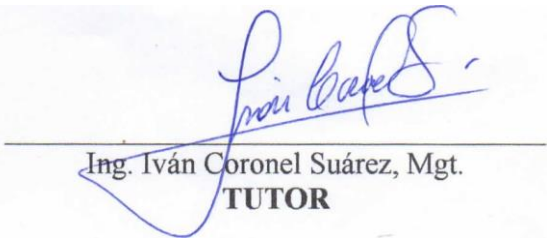
2023

UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

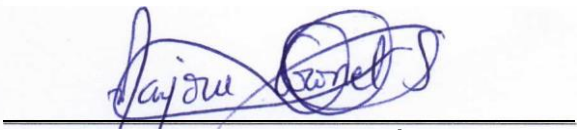


Ing. José Sánchez Aquino, Mgt.
DIRECTOR DE LA CARRERA



Ing. Iván Coronel Suárez, Mgt.
TUTOR

Lsi. Daniel Quirumbay Yagual, Mgt.
DOCENTE ESPECIALISTA



Ing. Marjorie Coronel Suárez Mgt.
DOCENTE GUÍA UIC

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por Panimboza Panchana Anthony Mauricio, como requerimiento para la obtención del título de Ingeniero en Tecnologías de la Información.

La Libertad, a los 02 días del mes de Agosto del año 2023

TUTOR

Ing. Iván Coronel Suárez Mgt.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
DECLARACIÓN DE RESPONSABILIDAD

Yo, **ANTHONY MAURICIO PANIMBOZA PANCHANA**

DECLARO QUE:

El trabajo de Titulación**, Implementación de un plan de acción para las buenas prácticas en la gestión de la seguridad de la información del departamento de tics de la Upse**, previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

La Libertad, a los 02 días del mes de Agosto del año 2023

EL AUTOR

ANTHONY PANIMBOZA PANCHANA

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado **Implementación de un plan de acción para las buenas prácticas en la gestión de la seguridad de la información del departamento de tics de la Upse**, presentado por el estudiante, Panimboza Panchana Anthony Mauricio fue enviado al Sistema Anti plagio, presentando un porcentaje de similitud correspondiente al 2%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.


CERTIFICADO DE ANÁLISIS
magister

TT_Panimboza_Panchana(1)

2% Similitudes

3% Texto entre comillas
< 1% similitudes entre comillas
< 1% Idioma no reconocido

Nombre del documento: TT_Panimboza_Panchana(1).docx
ID del documento: be5b0908bdf078fe4ac1acdfef6e7462dcc42501
Tamaño del documento original: 172,18 kB

Depositante: IVAN ALBERTO CORONEL SUAREZ
Fecha de depósito: 2/8/2023
Tipo de carga: interface
fecha de fin de análisis: 2/8/2023

Número de palabras: 10.296
Número de caracteres: 67.346

Ubicación de las similitudes en el documento:

TUTOR

Ing. Iván Coronel Suárez Mgt.

TUTOR

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **ANTHONY MAURICIO PANIMBOZA PANCHANA**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de artículo profesional de alto nivel con fines de difusión pública, además apruebo la reproducción de este artículo académico dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, a los 02 días del mes de Agosto del año 2023

EL AUTOR

ANTHONY PANIMBOZA PANCHANA

AGRADECIMIENTO

Le agradezco primeramente a mis padres que con su soporte incondicional hicieron posible que yo pueda cumplir con mis objetivos personales y académicos, que con su cariño y enseñanzas me inculcaron a nunca rendirme frente a los infortunios.

Tambien agradezco a mi Tutor que con dedicación y paciencia fue posible el desarrollo de este trabajo, gracias a sus palabras y correcciones he podido lograr llegar a esta instancia tan anhelada. Sus consejos los llevare siempre presente en mi carrera como profesional.

A todos los docentes que fueron parte durante mi vida académica les agradezco por transmitir sus conocimientos para poder estar aquí hoy y gracias por sus exigencias y por nunca dejar de confiar en mí.

A mis compañeros que ahora con orgullo llamo amigos y hermanos debo agradecerles el esfuerzo compartido, el tiempo y anécdotas, no solo quedaran en mi memoria sino tambien en mi corazón,

Por último, gracias Universidad por tu exigencia académica, pero que debido a eso se me permite obtener mi tan ansiado título. Agradezco a la directiva y su gestión, que debido a ellos las condiciones de adquirir conocimientos son de un alto nivel.

Anthony Mauricio, Panimboza Panchana

DEDICATORIA

Dedico este trabajo principalmente a Dios, por haberme dado la vida y permitirme el haber llegado hasta este momento tan importante de mi formación profesional. A mi madre, por ser el pilar más importante y por demostrarme siempre su cariño y apoyo incondicional sin importar nuestras diferencias de opiniones. A mi Tía y Abuela, a pesar de nuestra distancia física, siento que están conmigo siempre y aunque nos faltaron muchas cosas por vivir juntos, sé que este momento hubiera sido tan especial para ustedes como lo es para mí. A mi Hermano, a quien admiro mucho, gracias por compartir momentos significativos conmigo y por siempre estar dispuesto a escucharme y ayudarme en cualquier momento. A mi sobrina Yuribeth, porque te amo infinitamente. A mis compañeros, porque sin el equipo que formamos, no hubiéramos logrado esta meta.

Anthony Mauricio, Panimboza Panchana

RESUMEN

La Universidad UPSE enfrenta desafíos en la gestión de su información y seguridad debido a la falta de políticas y controles adecuados. El departamento de TIC es responsable de garantizar la integridad, confiabilidad y disponibilidad de la información, pero la ausencia de políticas de seguridad expone a la universidad a riesgos. La falta de control de acceso y medidas de seguridad física también aumenta las amenazas.

Es esencial implementar un plan de acción basado en buenas prácticas de seguridad de la información y cumplir con la norma ISO 27002 para proteger los activos de información de la universidad y abordar las deficiencias actuales en el departamento de TIC. Esto incluye garantizar el adecuado distanciamiento entre equipos, mantener la seguridad en el data center y considerar factores ambientales y de riesgo.

Palabras claves: Implementar, plan de acción, buenas prácticas

ABSTRACT

UPSE University faces challenges in managing its information and security due to the lack of adequate policies and controls. The ICT department is responsible for guaranteeing the integrity, reliability and availability of information, but the absence of security policies exposes the university to risks. The lack of access control and physical security measures also increases threats.

It is essential to implement an action plan based on good information security practices and comply with ISO 27002 to protect the university's information assets and address current deficiencies in the ICT department. This includes ensuring proper distancing between equipment, maintaining data center security, and considering environmental and risk factors.

Keywords: Implement, action plan, good practices.

INDICE

ÍNDICE DE FIGURA

ÍNDICE DE TABLA

CAPÍTULO I

1 FUNDAMENTACIÓN

1.1 ANTECEDENTES

La información y los sistemas de información cada vez se encuentran más expuestos a los riesgos como resultado del incremento en el intercambio de datos internos y externos, así como del mayor uso de redes abiertas [1]. Es importante garantizar la seguridad de la información para minimizar los riesgos y evitar daños a las empresas, por ello, surge la necesidad de implementar medidas apropiadas de seguridad de la información y una de las iniciativas de gestión de TI más cruciales es la gestión de seguridad de la información sistematizada [2].

En este contexto, surgió la norma ISO/IEC 27002 de alcance internacional, que se centra en las prácticas más adecuadas para administrar la seguridad de la información [3]. En la actualidad, esto es crucial para el desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI), que garantice la continuidad y el mantenimiento de los procedimientos de seguridad en concordancia con los objetivos estratégicos de la organización [4].

La Universidad Estatal Península de Santa Elena (UPSE) dentro de su estructura organizacional posee como función de soporte administrativo el departamento de Tecnología de la Información (TIC´S). Esta unidad está conformada por las áreas de soporte técnico, desarrollo, redes y telecomunicaciones [5].

A pesar del tiempo de creación de este departamento la seguridad física, ambiental y el control de acceso no reflejan el cumplimiento de las buenas prácticas de un sistema de gestión de la seguridad informática (SGSI). En el año 2018 a través de la Resolución N° 001-R-ADM-UPSE-2018, se aprobaron políticas de seguridad informática basadas en las normas ISO 27002, sin embargo, éstas se encuentran muy generalizadas y no han sido actualizadas [6].

En la investigación realizada se detectó que las áreas antes mencionadas del departamento de TIC´S no cuentan con un control de acceso a los usuarios externos debido a que los usuarios como docentes, estudiantes, administrativos, entre otros ingresan a las áreas causando riesgos o vulnerabilidades en la información alojada en los equipos físicos (computadoras, servidores, redes, etc.). Así mismo, es necesario verificar que los equipos físicos y humanos se encuentren implementados de manera

correcta, cumpliendo con el debido distanciamiento, ambientación y seguridad.

Por tal motivo, el presente proyecto se basa en la implementación de un plan de acción basado en la Norma ISO 27002 sección 9 y 11, que permitirá adquirir buenas prácticas en la gestión de la seguridad de la información del ambiente físico y control de acceso del departamento de TIC´S de la UPSE.

1.2 DESCRIPCIÓN DEL PROYECTO

Las políticas de seguridad de la UPSE son insuficientes para garantizar el control de acceso y espacio físico que debe tener el departamento de TIC´S, por esta razón, se propone implementar un plan de acción para las buenas prácticas del SGSI en la seguridad física, ambiental y control de acceso, que permitirá a los gestores de nivel jerárquico superior tomar acciones correctivas [7].

Para la ejecución del presente trabajo investigativo se establecen las siguientes fases:

Fase de recopilación de información

En esta fase se realizará una investigación cualitativa debido a que se utilizarán las técnicas de observación directa y entrevistas al personal.

Observación directa: se enfatiza por el hecho de que el investigador se encuentra presente en el lugar donde ocurre el evento sin intervenir ni perturbar el entorno [8], ya que, de lo contrario, los datos obtenidos no serían válidos [9]. Ejemplo: Identificar características de los niños en situación de calle [9]. Esta técnica se utilizará porque se hará un acercamiento a las áreas del departamento de TIC´S

Entrevistas: es una técnica de gran utilidad en la investigación cualitativa para recabar datos [10]; se define como una conversación que se propone un fin determinado distinto al simple hecho de conversar. Es un instrumento técnico que adopta la forma de un diálogo coloquial [11]. Esta técnica se la realizará al personal que labora en el departamento de TIC´S.

Fase de aplicación del baremo

Para el desarrollo de esta investigación se considera utilizar la ISO 27002 debido a que, las políticas de seguridad que tiene la UPSE se establecen en esta misma norma, lo que conlleva a que tenga fácil adaptabilidad. Las secciones de la norma consideradas para este proyecto son la 9 y 11 [4]:

Sección 9 – Seguridad física y del medio ambiente [3]

Los equipos e instalaciones de procesamiento de información crítica o sensible deben mantenerse en áreas seguras, con niveles y controles de acceso apropiados, incluyendo protección contra amenazas físicas y ambientales [3].

Sección 11 – Control de acceso [3]

El acceso a la información, así como a los recursos de procesamiento de la información y los procesos de negocios, debe ser controlado con base en los requisitos de negocio y en la seguridad de la información [3]. Debe garantizarse el acceso de usuario autorizado y prevenido el acceso no autorizado a los sistemas de información, a fin de evitar daños a documentos y recursos de procesamiento de la información que estén al alcance de cualquiera [3].

En esta fase se llevará a cabo los baremos establecidos en la norma para evaluar el departamento de TIC´S.

Fase de informe de resultados

Una vez aplicado el baremo se procederá a realizar un informe respecto a los resultados encontrados en la investigación.

Fase de construcción del plan de acción

Fundamentado en el informe se construirá un plan de acción que permita a los gestores tomar decisiones con respecto a los resultados encontrados y sugerir posibles soluciones.

1.3 OBJETIVOS DEL PROYECTO

1.3.1 OBJETIVO GENERAL

Implementar un plan de acción de buenas prácticas del SGSI mediante el estándar ISO 27002 sección 9 y 10 para el departamento de TIC´S de la UPSE

1.3.2 OBJETIVOS ESPECÍFICOS

- Recopilar información en el departamento de TIC´S a través de la observación directa y entrevista al director.
- Aplicar un baremo con base a la norma ISO 27002 sección 9 y 11 en el departamento de TIC´S.
- Generar un plan de acción basado en los resultados de la aplicación del baremo

1.4 JUSTIFICACIÓN DEL PROYECTO

La UPSE actualmente posee una gran cantidad de sistemas en el que fluye información relevante para la comunidad universitaria, a la vez, el departamento de TIC´S es el encargado de que el procesamiento de esa información cumpla con los principios básicos que son la integridad, confiabilidad y disponibilidad. El no tener políticas de seguridad que especifiquen el cuidado de estos activos incitan a que los mismos se encuentren vulnerables debido a que el personal del área y los usuarios que acceden a los activos de tecnología e información no tienen establecidos los requisitos y pautas de actuación necesarias para proteger el SGSI.

Las áreas del departamento de TIC´S no tienen un apropiado nivel y control de acceso a los sistemas y locaciones que procesan información crítica o sensible haciendo que se incrementen las amenazas en la información y seguridad física, además, la accesibilidad de la información a usuarios no autorizados podría resultar en posibles daños a documentos y recursos de procesamiento de información, accesibles para cualquier persona.

El espacio físico del departamento de TIC´S debe garantizar el correcto funcionamiento con respecto al distanciamiento entre equipos informáticos, data center, luminosidad, riesgos en el ambiente, etc.

La implementación de un plan de acción para las buenas prácticas del SGSI en el control de acceso y la seguridad física y ambiental permitirá realizar correctivos que coadyuven a proteger los activos de información de la universidad, identificando las falencias actuales en el departamento y rigiéndose a lo especificado en la norma ISO 27002.

El tema propuesto está alineado a los objetivos del Plan de Creación de Oportunidades al siguiente eje:

Directriz 1: Soporte territorial para la garantía de derechos.

Lineamiento territorial A. Acceso equitativo a servicios y reducción de brechas territoriales.

A4. Fortalecer la conectividad y el acceso a las TIC como una vía para mejorar el acceso a otros servicios [12].

Objetivos del eje Económico

Objetivo 5: Proteger a las familias, garantizar sus derechos y servicios, erradicar la pobreza y promover la inclusión social [12].

Política 5.5: Mejorar la conectividad digital y el acceso a nuevas tecnologías de la población

1.5 ALCANCE DEL PROYECTO

El presente proyecto se realizará en las áreas del departamento de TIC´S de la UPSE. Se basará en el SGSI en el control de acceso y la seguridad física y ambiental de la unidad.

El proyecto concluirá con un plan de acción basado en el resultado de la aplicación de la norma ISO 27002 sección 9 y 11 el mismo, que será entregado al director del departamento especificando las mejoras que se podrían llevar a cabo para las buenas prácticas del SGSI.

Las fases que se llevarán a cabo en esta investigación son las siguientes:

Fase 1: Recolección de información a través de revisión bibliográfica y documental del departamento de TIC´S, observación directa en las áreas que componen la unidad y entrevistas abiertas al personal que labora en el departamento.

Fase 2: Se aplicará el baremo establecido por la norma ISO 27002 en las secciones 9 y 11 para medir el uso de las buenas prácticas del SGSI.

Fase 3: Una vez aplicado el baremo se podrá realizar un informe de los resultados de la investigación

Fase 4: El plan de acción contendrá los lineamientos de la ISO 27002 correctivos para el departamento de TIC´S y serán entregados al gestor de la unidad.

El gestor del departamento será quien en conjunto a su equipo tome la decisión de aplicar las mejoras recomendadas.

CAPÍTULO 2

2 MARCO TEORÍCO Y METODOLOGÍA DEL PROYECTO

2.1 MARCO TEÓRICO

Con base a la revisión bibliográfica se referencia los siguientes trabajos investigativos que coadyuvaran en el desarrollo del presente proyecto:

2.1.1 Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000

Los autores Valencia y Orozco en su investigación propusieron una metodología para la implementación de un SGSI basado en la familia de normas de la ISO/IEC 27000 [13].

En esta investigación científica se enfocaron en cuatro normas que son: la ISO 27001, ISO 27002, ISO 27005 y ISO 27003. Por lo que, los autores expresan que "Hay varias formas de implementar un Sistema de Gestión de Seguridad de la Información (SGSI) en una organización. Sin embargo, para aumentar las posibilidades de éxito y reducir la incertidumbre en los resultados, es crucial adoptar un enfoque sistémico que aborde de manera integral los elementos que conforman este sistema" [13].

Los investigadores proponen una metodología de cinco fases descritas a continuación [13]:

Fase 1: Aprobación de la Dirección para iniciar el proyecto, Fase 2: Definir el alcance, los límites y la política del SGSI, Fase 3: Análisis de los requisitos de seguridad de la información, Fase 4: Valoración de riesgos y planificar el tratamiento de riesgos, Fase 5: Diseñar el SGSI [13].

2.1.2 Análisis e implementación de la seguridad de la información del centro de datos de la Universidad Nacional de la Amazonía Peruana bajo la norma 27002

El autor García realizó esta investigación con la finalidad de conocer las vulnerabilidades de la información de la UNAP en consecuencia a la falta de aplicación de controles de seguridad del centro de datos. Para llevar a cabo esta investigación el autor considera necesario utilizar los controles de seguridad de la norma ISO 27002 [14].

García eligió esta norma porque indica que "las Normas ISO/IEC 27002 permitirá conocer las vulnerabilidades existentes en el manejo de la información física, así como la

que está contenida en los sistemas de procesamiento de información, de tal forma que se puedan tomar acciones preventivas y correctivas dentro de la empresa, para evitar que se lleguen a comprometer datos confidenciales" [14].

En el transcurso del proyecto se observa que el autor hace una evaluación del centro de datos de la UNAP basado en la ISO 27002, en donde se evidencia el nivel de cumplimiento en los controles de la norma. Así mismo, concluyó que las áreas críticas reflejan potenciales índices de riesgos con respecto a la seguridad de la información y entre sus recomendaciones se establece la necesidad de designar un responsable de la seguridad informática del centro [14].

2.1.3 Análisis e implementación de la norma ISO 27002 para el departamento de sistemas de la Universidad Politécnica Salesiana sede Guayaquil

Esta investigación desarrollada por los autores Daniel Romo V. y Joffre Valarezo C. fue aplicada en el departamento de sistemas de la universidad, debido a que, los investigadores detectaron la falta de políticas o normas de seguridad de la información y los problemas que se derivaban del mismo [15].

Los autores de este proyecto crearon un manual de políticas de seguridad dirigido a docentes, administrativos y externos, manifestando que "la finalidad del proyecto es proporcionar instrucciones específicas sobre cómo proteger los activos de la Universidad Politécnica Salesiana ya sean estos computadores de la organización (conectados o no), como toda la información guardada en ellos" [15].

Para el desarrollo de estas políticas se fundamentaron en los controles de la ISO 27002 en sus once dominios concluyendo que al aplicar el manual creado por los investigadores se podrían minimizar los riesgos asociados a los activos de la universidad [15].

2.2 MARCO CONCEPTUAL

2.2.1 Seguridad de la información

Es la práctica que permite proteger la información y los datos del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados [16]. Implica implementar medidas y estrategias para garantizar la confidencialidad, integridad y disponibilidad de la información, así como protegerla contra diversas amenazas, como piratas informáticos, malware, violaciones de datos y robo físico [16].

Los principales objetivos de la seguridad de la información son [17]:

- Confidencialidad: Garantizar que la información confidencial sea accesible solo para personas o entidades autorizadas y permanezca confidencial.
- Integridad: Mantener la precisión, integridad y confiabilidad de la información a lo largo de su ciclo de vida y evitar modificaciones no autorizadas.
- Disponibilidad: Garantizar que los usuarios autorizados tengan acceso oportuno e ininterrumpido a la información y los recursos del sistema cuando sea necesario.
- Autenticación: Verificación de la identidad de los usuarios y entidades para evitar el acceso no autorizado.
- Autorización: Concesión de privilegios y permisos adecuados a los usuarios en función de sus funciones y responsabilidades.
- No repudio: Garantizar que el remitente no pueda negar el origen y la integridad de la información.

La seguridad de la información se basa en una combinación de controles técnicos, de procedimiento y administrativos, incluidos el cifrado, los controles de acceso, los cortafuegos, los sistemas de detección de intrusos, las políticas de seguridad, los programas de formación y concienciación, los planes de respuesta a incidentes y las evaluaciones periódicas de seguridad [18]. Estas medidas ayudan a mitigar los riesgos, proteger contra las amenazas y salvaguardar la información confidencial del acceso no autorizado o el uso indebido [19].

2.2.2 Sistema de gestión de seguridad de la información (SGSI)

Es un conjunto de políticas, procedimientos, normas, y herramientas que una organización utiliza para controlar, proteger y asegurar la información y los sistemas de información que maneja [20].

El objetivo principal de un SGSI es garantizar la confidencialidad, integridad y disponibilidad de la información, es decir, protegerla contra el acceso no autorizado, la modificación no autorizada y la pérdida de disponibilidad [13].

Un SGSI generalmente sigue un enfoque basado en el riesgo y se adapta a las necesidades específicas de la organización. La implementación de un SGSI implica la identificación y evaluación de los riesgos de seguridad de la información, la definición de controles de seguridad adecuada, la implementación y operación de esos controles, y la monitorización

y revisión continua del sistema para asegurarse de que sea efectivo y esté actualizado [21].

Un SGSI puede ser certificado por terceros para demostrar que cumple con estándares reconocidos a nivel internacional, como la norma ISO/IEC 27001 [22].

2.2.3 Buenas prácticas de la seguridad de la información

Consiste en la creación y aplicación de políticas y lineamientos que direccionen el desarrollo de la seguridad de la información y los principios de acción de los entes que tienen acceso o responsabilidades sobre la información sensible en la empresa [23].

Las empresas generalmente optan por adquirir buenas prácticas referenciando marcos públicos de trabajo o normas tales como: ISO/IEC 2000, ITIL, COBIT, CMMI, entre otros [24]

Entre los beneficios de las buenas prácticas en la gestión de la información se destacan los siguientes [24]:

- Los objetivos de TI estarán concatenados a los objetivos del negocio
- Reducción de riesgos en los servicios de TI
- Cuantificación del valor real de los servicios de TI
- Fortalecimientos en la comunicación interna del departamento de TI al usuario o áreas externas
- Mayor adaptabilidad a los cambios del negocio
- Minimización de impacto en las fallas de los servicios
- Capacidad para la toma de decisiones con base a los indicadores de negocio y de TI
- Aumento en la satisfacción al cliente

2.2.4 ISO (Organización Internacional para la Estandarización)

Fue fundada el 23 de febrero de 1947 y tiene el fin de fomentar la aplicación de normas comerciales, industriales y de propiedad en todo el mundo [25]

Es un grupo de organismos nacionales dedicadas a desarrollar normas internacionales, cada miembro de la ISO es el principal organismo de normalización de su país, debido a que, ellos proponen la creación de nuevas normas, intervienen en su desarrollo y brindan

su contingente en unión de la Secretaría General de la ISO [25].

En la Figura 1, se muestran las normas que utiliza la ISO, considerando que cada norma apoya a las demás como bloques en una pared [25].

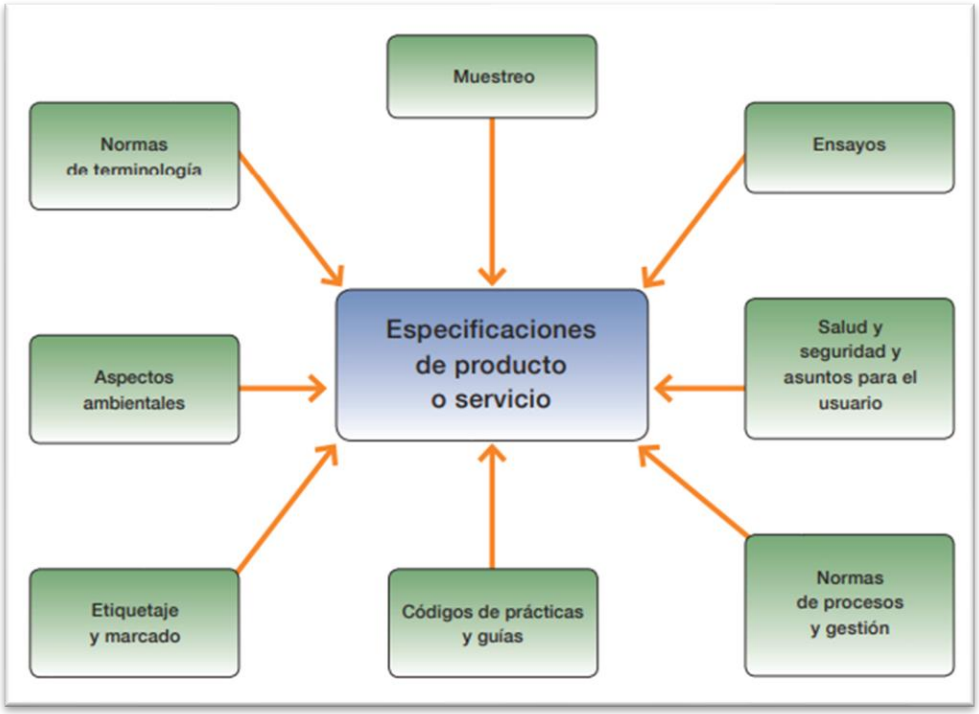


Figura 1: Serie de normas *[25]*

Las normas ISO más utilizadas son [26]:

Calidad	Medio Ambiente	Riesgos y seguridad	Responsabilidad social
ISO 9001	ISO 14001	ISO 22000	SA 8000
ISO 9004	ISO 50001	ISO 22301	ISO 26000
ISO IEC 17025		ISO IEC 27001	
ISO TS 16949		ISO 28000	
Sistemas Integrados de Gestión		ISO 31000	
		ISO 37001	
		ISO 37301	
		ISO 39001	
		ISO 45001	

Tabla 1: Listado de normas ISO

2.2.5 ISO 27002

Fue publicada en julio de 2005, reemplazó a la norma ISO/IEC 17799:2000, que

actualmente se encuentra despublicada. Aunque inicialmente tenía el número ISO/IEC 17799, a esta norma se le asignó el número ISO/IEC 27002 para que sea miembro de la serie de normas de la ISO 27000 [2].

La ISO/IEC 27002:2005 (ISO27002) se centra en el código internacional de mejores prácticas para el enfoque orientado a la seguridad de la información. Los requisitos de seguridad de la información deben identificarse mediante una evaluación metódica del riesgo de seguridad [27].

El principal objetivo de la ISO 27002 es "establecer directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización" [3].

A continuación se enlista las principales distribuciones de la norma en las secciones correspondientes a los controles de seguridad de la información, los mismos, que pueden ser referenciados por las entidades en la creación del SGSI [28]:

- **Sección 5 – Política de Seguridad de la Información**

La organización debe desarrollar políticas de seguridad de la información, la cual debe incluir ideas de seguridad de la información, un marco para establecer las metas y tipos de control, así como el compromiso de la gerencia con la política, entre muchas otras cosas [28].

- **Sección 6 – Organización de la Seguridad de la Información**

Se debe establecer una estructura para administrar de manera efectiva la seguridad de la información antes de que se pueda implementar en un negocio. Para lograr esto, los representantes de la organización que tienen funciones claramente definidas y están comprometidos con la protección de la información confidencial deben coordinar los esfuerzos de seguridad de la información [28].

- **Sección 7 – Gestión de activos**

Para estructurar y luego administrar un inventario, primero se deben identificar y categorizar los activos. También deben cumplir con las normas escritas que describen los usos aceptables de esos activos [28].

- **Sección 8 – Seguridad en recursos humanos**

El propósito de esta sección es reducir el riesgo de robo, fraude o uso indebido de

recursos. Y cuando los empleados trabajan para una empresa, deben ser conscientes no solo de sus responsabilidades y obligaciones, sino también de las amenazas asociadas con la seguridad de la información [28].

- **Sección 9 – Seguridad física y del medio ambiente**

Los equipos e instalaciones de procesamiento de información crítica o confidencial deben mantenerse en lugares seguros con un nivel adecuado de acceso y control, incluida la protección contra amenazas físicas y ambientales [28].

- **Sección 10 – Seguridad de las operaciones y comunicaciones**

Es crucial describir claramente los procesos y roles involucrados en la gestión y ejecución de todos los recursos de procesamiento de información. Esto implica administrar servicios subcontratados, programar los recursos del sistema para reducir la probabilidad de fallas, desarrollar procesos para crear copias de respaldo y recuperarlas, y administrar de manera segura las redes de comunicación [28].

- **Sección 11 – Control de acceso**

Según las necesidades comerciales y la seguridad de la información, se debe administrar el acceso a la información, los recursos de procesamiento de la información y los procesos comerciales. Para evitar daños a los documentos de acceso público y los recursos de procesamiento de información, se debe garantizar el acceso de usuarios autorizados y se debe evitar el acceso no autorizado a los sistemas de información [28].

- **Sección 12 – Adquisición, desarrollo y mantenimiento de sistemas**

Previo a su creación y/o implementación, se deben determinar y acordar las necesidades de seguridad de los sistemas de información, permitiendo el uso de técnicas criptográficas para mantener su integridad, confidencialidad y autenticidad [28].

- **Sección 13 – Gestión de incidentes de seguridad de la información**

Para garantizar que los incidentes de seguridad de la información se notifiquen y solucionen lo antes posible, se deben desarrollar procesos formales de registro y escalamiento, e informar a los trabajadores, proveedores y terceros sobre los protocolos para notificar los eventos de seguridad de la información [28].

- **Sección 14 – Gestión de continuidad del negocio**

Para evitar la interrupción de las operaciones corporativas y garantizar que las funciones críticas se restablezcan rápidamente, se deben crear e implementar planes de continuidad del negocio [28].

- **Sección 15 – Conformidad**

Es fundamental evitar infringir cualquier ley, ya sea penal o civil, así como cualquier legislación, regla u obligación contractual que lo justifique, incluido cualquier estándar para la seguridad de la información. Para confirmar su cumplimiento y adhesión a las normas legales y reglamentarias, la empresa podrá, si es necesario, designar un consultor profesional [28].

2.3 METODOLOGÍA DEL PROYECTO

2.3.1 Metodología de investigación

El presente proyecto se basa en una investigación exploratoria, debido a que, este tipo de estudios tiene como objetivo principal captar una perspectiva general del problema y dividirlo en subproblemas, para así generar criterios que permitan dar prioridad a casos específicos [29].

Esta investigación se utiliza para los siguientes propósitos [29]:

- Formular problemas para estudios más precisos o para desarrollo de hipótesis.
- Establecer prioridades para futuras investigaciones.
- Recopilar información acerca de un problema que luego se dedica a un estudio especializado particular.
- Aumentar el conocimiento respecto del problema.
- Aclarar conceptos.

En la UPSE existe un documento generalizado de políticas de seguridad basadas en las ISO 27002, sin embargo, no se profundiza respecto al control de acceso ni a la seguridad física y ambiental en el departamento de TIC´S, ni se ha realizado un estudio que verifique si se están aplicando los lineamientos de esta norma.

Es necesario que en este proyecto también se realice una investigación diagnóstica, que nos permitirá tener la interpretación de una realidad para definir líneas y estrategias de acción [30].

Por lo tanto, este estudio permitirá profundizar el tema utilizando técnicas de recopilación de información como la revisión bibliográfica y documental del departamento de TIC´S, observación directa y entrevistas al personal.

En el desarrollo de este trabajo investigativo se ha identificado una variable:

- ✓ Implementar el 100% del baremo de la ISO 27002 respecto al control de acceso y seguridad física y ambiental

2.3.2 Técnicas de recolección de información

Para obtener la información necesaria en este proyecto investigativo se utilizaron las técnicas de revisión bibliográfica y documental, observación directa y entrevistas al personal del departamento de TIC´S.

Se realizó una revisión esencialmente a los contenidos de la ISO 27002 para tener una amplitud con respecto a las dimensiones/secciones y matrices del SGSI. Así mismo, se constató la documentación que posee el departamento de TIC´S con respecto al manual de procesos, políticas de seguridad, estructura orgánica, análisis de riesgo, entre otros, para tener un estudio situacional de la unidad.

La técnica de observación directa se la realizó en las áreas que componen el departamento de TIC´S, esto será de gran utilidad para entender los procesos y comportamientos que se llevan a cabo, tanto del personal interno como la relación con los usuarios externos. Además permitió tener un bosquejo de la estructura física del departamento.

Es fundamental tener un diálogo con el personal que labora directamente en esta unidad, por lo que, se realizó entrevistas abiertas que permitieron conocer los criterios de los involucrados en esta investigación.

2.3.3 Metodología

Para llevar a cabo el desarrollo del proyecto se han establecido cuatro fases fundamentales que permitirán alcanzar el objetivo de esta investigación:

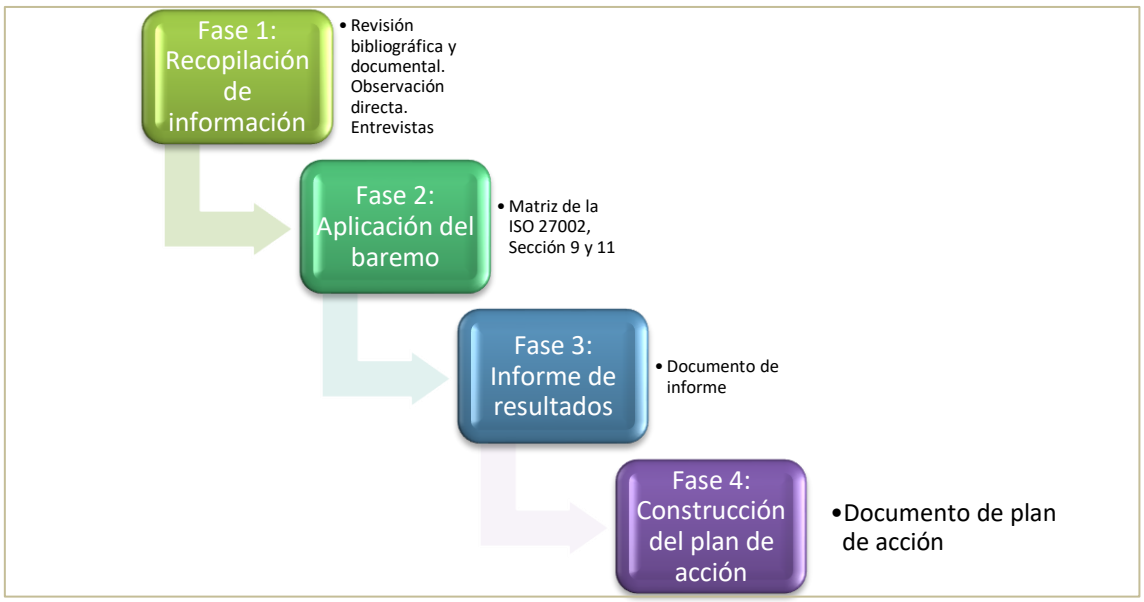


Figura 2: Metodología de desarrollo

2.3.4 Análisis de la entrevista

En esta sección se realiza un análisis de las respuestas generadas por el director del departamento de TIC´S. Ver Anexo 1.

PREGUNTA 1: ¿Cuántas áreas tiene el departamento de TIC´S y qué funciones tiene cada una?

El director menciona que el departamento tiene la siguiente estructura:

Figura 3: Estructura organizacional del departamento de TIC´S

PREGUNTA 2: ¿La UPSE tiene establecido sus políticas de seguridad?

El entrevistado comenta que si existen políticas de seguridad en la UPSE pero que se encuentran más orientadas al usuario

PREGUNTA 3: ¿Hace cuánto tiempo fueron creadas estas políticas?

De acuerdo con lo expresado por el director, las políticas fueron creadas en el año 2018

PREGUNTA 4: ¿Considera usted que las políticas de seguridad de la UPSE son óptimas para la protección de la información de la organización?

El entrevistado manifestó que considera que se debe elaborar un nuevo documento de políticas de seguridad, debido a que, las actuales se encuentran más orientadas al usuario y están generalizadas. Así mismo, indicó que las políticas necesitan ser modificadas, normadas y aprobadas por el equipo experto.

PREGUNTA 5: ¿Cuál es el plan de acción que tiene el departamento de TIC´S para la prevención, mitigación y atención de riesgos?

El director expresó que actualmente el departamento no tiene de manera oficial un plan de acción, pero que se realizan a través de solicitudes y oficios de la dirección a las áreas correspondientes.

PREGUNTA 6: ¿Cuál es la metodología que utilizan ustedes para el análisis de

riesgo?

En esta pregunta el entrevistado indicó que no existe un documento oficial de análisis de riesgo. Esto es preocupante, debido a que, no se tiene una evaluación del impacto que puede ocasionar un evento.

Al no existir el análisis de riesgo, no se pudieron realizar las siguientes preguntas concernientes a este tema.

PREGUNTA 10: ¿En qué documento se encuentran plasmadas las reglas y normas para el control de acceso en áreas críticas como el área de desarrollo de software, área de servidores, etc.?

El director reconoce que se debe trabajar en este tema por lo que no existe tampoco un documento de regulación para el control de acceso. Sin embargo, si se han realizado socializaciones a los miembros de la comunidad universitaria sobre la seguridad informática.

De igual manera que la anterior pregunta, al no tener este documento no se pudieron realizar las siguientes preguntas concernientes a este tema.

PREGUNTA 12: ¿Cuáles son las técnicas que ustedes utilizan para dar seguridad en el procesamiento de la información? (por ejemplo: tipo de encriptación, seguridad en redes, etc.)

El entrevistado explicó que manejan varias técnicas, entre esas la separación de redes por vlan, procesos de encriptación, firewalls, entre otros.

PREGUNTA 13: ¿Basados en qué regularización crearon la estructura física de cada área del departamento, especialmente el data center?

El entrevistado desconoce del tema pero indica que el proveedor del data center si se basó en una norma o estandarización.

PREGUNTA 14: ¿Cómo se concatenan las políticas de seguridad actuales con los objetivos institucionales?

Indica que para la concatenación es necesario como lo dijo anteriormente, modificar estas políticas de seguridad y difundirlas a la comunidad universitaria.

PREGUNTA 15: ¿Considera útil la creación de un plan de acción para las buenas prácticas en el SGSI? ¿Por qué?

El entrevistado considera muy útil no sólo la creación del plan de acción para las buenas prácticas sino también el resto de documentación que normalice la seguridad de la información en la institución como la modificación y actualización de las políticas de seguridad, la creación de la documentación de análisis de riesgo, etc.

2.3.5 Conclusión de la entrevista

Basado en las respuestas obtenidas por el entrevistado se concluye que el departamento de TIC´S carece de documentación normada para la seguridad de la información, esto a su vez es preocupante porque actualmente los procesos de la universidad se realizan de manera automatizada a través de los sistemas creados por el departamento.

Las políticas de seguridad que se encuentran vigentes en la institución, de acuerdo con el criterio del director del departamento, están generalizadas e incompletas y deben ser actualizadas y concatenadas con los objetivos institucionales.

2.4 COSTO DE IMPLEMENTACIÓN

Para el desarrollo del presente proyecto se requieren los siguientes recursos:

Recursos de software

Ítem	Descripción	Cantidad	Costo Unitario	Costo Total
1	ISO/IEC 27002:2022	1	$213,31	$213,31
TOTAL				$213,31

Tabla 2: Recursos de software

Recursos de hardware

Ítem	Descripción	Cantidad	Costo Unitario	Costo Total
1	Laptop Procesador Core i7 Memoria RAM 4GB DDR 1 TB Mín. Décima Generación	1	$980,00	$980,00
2	Impresora Tecnología de inyección de tinta continua Resolución mín. de 5760 x 1440 dpi	1	$400,00	$400,00

	Incluye escáner y área de digitalización			
3	Disco Duro Externo Capacidad 1 TB Compatibilidad S.O.: Windows, MAC, Linux	1	$80,00	$80,00
TOTAL				$1.460,00

Tabla 3: Recursos de hardware

Recursos humanos

Ítem	Descripción	Cantidad	Duración	Costo Unitario	Costo Total
1	Auditor de calidad certificado en ISO	1	2 meses	$4.000,00	$8.000,00
2	Experto en seguridad informática	1	2 meses	$2.250,00	$4.500,00
3	Experto en gestión organizacional	1	1 mes	$1.000,00	$2.000,00
	TOTAL				$14.500,00

Tabla 4: Recursos humanos

Teniendo en consideración que el proyecto se ha desarrollado como un trabajo que se está realizando en proceso de, los recursos serán asumidos por el autor. Por lo consiguiente, el costo real al departamento será de $0,00 dólares.

CAPÍTULO 3

3 PROPUESTA

3.1 ESTRUCTURACIÓN DEL BAREMO

Para el desarrollo del presente proyecto fue fundamental estructurar una matriz que permita evaluar la seguridad física y del medio ambiente, así como el control de acceso del departamento de TIC´S.

Esta matriz fue diseñada con base a los controles establecidos en la ISO 27002 de las secciones 9 y 11.

En el Anexo 2 se visualiza el baremo desarrollado respecto a la seguridad física y del medio ambiente. De la misma manera, en el Anexo 3 se establece el baremo para el control de acceso.

3.2 APLICACIÓN DEL BAREMO

Los baremos presentados anteriormente fueron desarrollados en el departamento de TIC´S, a través de la técnica de observación directa y fundamentados en la entrevista que se le realizó al director (Ver Tabla 6 y Tabla 7).

9. CONTROL DE ACCESOS.						
9.1 Requisitos de negocio para el control de accesos.						
Control	**Descripción**	**Métrica**	**SI**	**NO**	**TALVEZ**	**OBSERVACIONES**
9.1.1 Política de control de accesos [31].	Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización [31].	Porcentaje de sistemas y aplicaciones corporativas para los que los "propietarios" adecuados han [31]: (a) sido identificados, (b) aceptado formalmente sus responsabilidades, (c) llevado a cabo -o encargado- revisiones de accesos y seguridad de aplicaciones, basadas en riesgo y (d) definido las reglas de control de acceso basadas en roles.			X	Se evidencia un documento de políticas de seguridad en la institución pero no existe el documento específico para el control de acceso
9.1.2 Control de acceso a las redes y servicios asociados [31].	Se debería proveer a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar [31].		X			
9.2 Gestión de acceso de usuario.						
Control	**Descripción**	**Métrica**	**SI**	**NO**	**TALVEZ**	**OBSERVACIONES**
9.2.1 Gestión de altas/bajas en el registro de usuarios [31].	Debería existir un procedimiento formal de alta y baja de usuarios con objeto de habilitar la asignación de derechos de acceso [31].	Tiempo medio transcurrido entre la solicitud y la realización de peticiones de cambio de accesos y número de solicitudes de cambio de acceso cursadas en el mes anterior (con análisis de tendencias y comentarios acerca de cualquier pico / valle (p. ej., "Implantada nueva aplicación financiera este mes") [31].			X	Existe el procedimiento de altas/bajas de usuarios pero no se encuentra formalizado. Existe la asignación o revocación de derechos pero no se encuentra formalizado. Se pudo observar que ex estudiantes de la institución aún tienen accesos a sus correos institucionales
9.2.2 Gestión de los derechos de acceso asignados a usuarios [31].	Se debería de implantar un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios [31].				X	

9.2.3 Gestión de los derechos de acceso con privilegios especiales [31].	La asignación y uso de derechos de acceso con privilegios especiales debería ser restringido y controlado [31].		X			
9.2.4 Gestión de información confidencial de autenticación de usuarios [31].	La asignación de información confidencial para la autenticación debería ser controlada mediante un proceso de gestión controlado [31].		X			
9.2.5 Revisión de los derechos de acceso de los usuarios [31].	Los propietarios de los activos deberían revisar con regularidad los derechos de acceso de los usuarios [31].		X			
9.2.6 Retirada o adaptación de los derechos de acceso [31].	Se deberían retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio [31].				X	
9.3 Responsabilidades del usuario.						
Control	**Descripción**	**Métrica**	**SI**	**NO**	**TALVEZ**	**OBSERVACIONES**

9.3.1 Uso de información confidencial para la autenticación [31].	Se debería exigir a los usuarios el uso de las buenas prácticas de seguridad de la organización en el uso de información confidencial para la autenticación [31].	Porcentaje de descripciones de puesto de trabajo que incluyen responsabilidades en seguridad de la información [31]: (a) totalmente documentadas y (b) formalmente aceptadas.	X			Se firma un acuerdo de confidencialidad entre el empleado y el empleador

9.4 Control de acceso a sistemas y aplicaciones.

Control	Descripción	Métrica	SI	NO	TALVEZ	OBSERVACIONES
9.4.1 Restricción del acceso a la información [31].	Se debería restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación con la política de control de accesos definida [31].	Porcentaje de soportes de backup o archivo que están totalmente encriptados [31].		X		Se observó que usuarios externos (estudiantes, administrativos, docentes) ingresan a las áreas críticas del departamento. No hay un control en la instalación de software, especialmente en los laboratorios de informática.
9.4.2 Procedimientos seguros de inicio de sesión [31].	Cuando sea requerido por la política de control de accesos se debería controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de log-on [31].		X			
9.4.3 Gestión de contraseñas de usuario [31].	Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar contraseñas de calidad [31].		X			
9.4.4 Uso de herramientas	El uso de utilidades software que podrían ser capaces de			X		

de administración de sistemas [31].	anular o evitar controles en aplicaciones y sistemas deberían estar restringidos y estrechamente controlados [31].					
9.4.5 Control de acceso al código fuente de los programas [31].	Se debería restringir el acceso al código fuente de las aplicaciones software [31].		X			

Tabla 5: Evaluación del baremo para el control de accesos

11. SEGURIDAD FÍSICA Y AMBIENTAL.						
11.1 Áreas seguras.						
Control	**Descripción**	**Métrica**	**SI**	**NO**	**TALVEZ**	**OBSERVACIONES**
11.1.1 Perímetro de seguridad física [32].	Se deberían definir y utilizar perímetros de seguridad para la protección de las áreas que contienen información y las instalaciones de procesamiento de información sensible o crítica [32].	Informes de inspecciones periódicas de seguridad física de instalaciones, incluyendo actualización regular del estado de medidas correctivas identificadas en inspecciones previas que aún estén pendientes [32].		X		No se observa señaléticas que ni nada que defina un perímetros de seguridad física. No se observan controles de entrada que garantice el ingreso de personal autorizado en las áreas. No existe documentación de control de riesgo ni de medidas correctivas.
11.1.2 Controles físicos de entrada [32].	Las áreas seguras deberían estar protegidas mediante controles de entrada			X		

	adecuados para garantizar que solo el personal autorizado dispone de permiso de acceso [32].					
11.1.3 Seguridad de oficinas, despachos y recursos [32].	Se debería diseñar y aplicar un sistema de seguridad física a las oficinas, salas e instalaciones de la organización [32].			X		
11.1.4 Protección contra las amenazas externas y ambientales [32].	Se debería diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes [32].			X		
11.1.5 El trabajo en áreas seguras [32].	Se deberían diseñar y aplicar procedimientos para el desarrollo de trabajos y actividades en áreas seguras [32].			X		
11.1.6 Áreas de acceso público, carga y descarga [32].	Se deberían controlar puntos de acceso a la organización como las áreas de entrega y carga/descarga (entre otros) para evitar el ingreso de personas no autorizadas a las dependencias aislando estos puntos, en la medida de lo posible, de las instalaciones de			X		

	procesamiento de información [32].					
11.2 Seguridad de los equipos						
Control	**Descripción**	**Métrica**	**SI**	**NO**	**TALVEZ**	**OBSERVACIONES**
11.2.1 Emplazamiento y protección de equipos [32].	Los equipos se deberían emplazar y proteger para reducir los riesgos de las amenazas y peligros ambientales y de oportunidades de acceso no autorizado [32].	Número de chequeos (a personas a la salida y a existencias en stock) realizados en el último mes y porcentaje de chequeos que evidenciaron movimientos no autorizados de equipos o soportes informáticos u otras cuestiones de seguridad [32].			X	Se observó que no todos los equipos se encuentran protegidos de amenazas y peligros ambientales. No existen políticas de puesto de trabajo.
11.2.2 Instalaciones de suministro [32].	Los equipos deberían estar protegidos contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos de apoyo [32].		X			
11.2.3 Seguridad del cableado [32].	Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se deberían proteger contra la intercepción, interferencia o posibles daños [32].		X			
11.2.4 Mantenimiento de los equipos [32].	Los equipos deberían mantenerse adecuadamente con el objeto de garantizar su disponibilidad e integridad continuas [32].		X			

11.2.5 Salida de activos fuera de las dependencias de la empresa [32].	Los equipos, la información o el software no se deberían retirar del sitio sin previa autorización [32].		X			
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones [32].	Se debería aplicar la seguridad a los activos requeridos para actividades fuera de las dependencias de la organización y en consideración de los distintos riesgos [32].		X			
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento [32].	Se deberían verificar todos los equipos que contengan medios de almacenamiento para garantizar que cualquier tipo de datos sensibles y software con licencia se hayan extraído o se hayan sobrescrito de manera segura antes de su eliminación o reutilización [32].		X			
11.2.8 Equipo informático de usuario desatendido [32].	Los usuarios se deberían asegurar de que los equipos no supervisados cuentan con la protección adecuada [32].	Informes de inspecciones periódicas a los equipos, incluyendo actividades para la revisión de rendimiento, capacidad, eventos de seguridad y limpieza de los diversos componentes (aplicaciones,		X		
11.2.9 Política de puesto de	Se debería adoptar una política de puesto de			X		

trabajo despejado y bloqueo de pantalla [32].	trabajo despejado para documentación en papel y para medios de almacenamiento extraíbles y una política de monitores sin información para las instalaciones de procesamiento de información [32].	almacenamiento, CPU, memoria, red, etc.) [32].				

Tabla 6: Evaluación del baremo para la seguridad física y ambiental

3.2.1 Informe de resultados

Se realizó la aplicación del baremo teniendo los siguientes resultados:

- **Control de accesos**

En la aplicación de la matriz del control de acceso se pudo evidenciar que la UPSE tiene en su sitio web con Resolución N° 001-R-ADM-UPSE-2018 sobre la aprobación de políticas de seguridad, sin embargo, no posee un documento específico sobre las políticas de control de accesos y en el reglamento general solo se encontró un ítem que trata sobre "Controles de Acceso Lógicos".

A pesar de no existir las políticas de control de acceso, el departamento posee un orden en la distribución e identificación de accesos a las redes y servicios de red al personal autorizado, lo que es muy importante para evitar infiltrados en la red.

El departamento de TIC´S posee un sistema para gestión de altas/bajas de usuarios pero no es un procedimiento que se encuentre formalizado. En varias ocasiones no se lleva un control adecuado de usuarios, por ejemplo, existen exestudiantes que aún poseen cuentas en sus correos institucionales. A pesar de que existe esta falencia, tienen un cuidado especial en la gestión de los derechos de acceso con privilegios especiales y esta función ha sido asignada a un ente del equipo quien es responsable de verificar que se asigne correctamente estos perfiles.

La universidad tiene un acuerdo de confidencialidad que es firmado por los contratados, indispensablemente del área al que se va a desempeñar, para asegurar el correcto uso de la información crítica de la institución.

En la visita que se realizó al departamento de TIC´S se pudo observar que entes externos a esta área como estudiantes, administrativos, docentes tenían acceso a áreas como la de desarrollo, lo que causa gran preocupación debido a que allí se maneja información de gran relevancia, además es la encargada de crear los sistemas de la universidad, y al no tener restricciones en el acceso se vuelve vulnerable a cualquier ataque informático o daños en su infraestructura tecnológica.

Los sistemas desarrollados por el departamento hacen que el usuario ingrese contraseñas seguras, además notifica al correo institucional del usuario cada inicio de sesión para verificar la autenticidad. Cabe destacar que la infraestructura de programación que utilizan asegura que el código fuente sea restringido.

- **Seguridad física y ambiental**

Las áreas que conforman el departamento de TIC´S tienen gran cantidad de equipos e

instalaciones de procesamiento de información crítica o sensible, por lo que, éste es el centro de captación y procesamiento de la información que fluye en la institución. Existe un espacio designado para el Data Center, otro para el área de desarrollo y de soporte, sin embargo, estos espacios no poseen perímetros de seguridad física ni señaléticas que indiquen las restricciones de personal o cuidados especiales en las áreas.

Otra de las preocupaciones en esta visita fue que no se posee una documentación de análisis de riesgos, por lo que, no se pueden valorar los impactos de daños ni tener un plan de medidas correctivas, reactivas ni preventivas.

Los equipos informáticos del departamento tienen su sistema de alimentación ininterrumpida en casos de fallos eléctricos, así mismo, a través de canaletas y cielos raso han sido implementado el cableado de red y eléctrico, lo que es categorizado como una buena práctica.

A través de la dirección departamental se planifican los mantenimientos periódicos a los equipos informáticos con el fin de garantizar la disponibilidad e integridad de estos, incluso si el equipo se encuentra obsoleto se da de baja y se solicita la renovación de este.

Para la movilización de equipos se realiza un procedimiento a través del departamento de activo fijo para registrar el traslado con firmas de los responsables.

3.3 DISEÑO DEL PLAN DE ACCIÓN

En consideración al informe de resultados de la aplicación del baremo, se establece la creación de un plan de acción que permita sugerir al encargado del departamento de TIC´S mejoras con relación al control de acceso y a la seguridad física y ambiental. Por tal motivo, se propone el siguiente plan de acción:

PLAN DE ACCIÓN: CONTROL DE ACCESOS				
Tema: Requisitos de negocio para el control de acceso			Subtema 1: Política de control de acceso	
Recomendación: Crear, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la UPSE.				
Medidas sugeridas	**Acciones estratégicas**	**Indicadores**	**Responsables**	**Plazos**
Fortalecer las políticas de seguridad que existen en la universidad	• Realizar un listado de los activos de la institución • Realizar un análisis de riesgos para categorizar los impactos de cada activo • Crear una comisión de expertos para la revisión de las políticas actuales y poder evaluar su desempeño • Con base al análisis de riesgo crear nuevas políticas de seguridad que permitan fortalecer las existentes • Difundir por los canales de comunicación las políticas de seguridad de la UPSE • Socializar las políticas de seguridad en grupos de docentes, administrativos, estudiantes y autoridades	• Informe de activos de la UPSE • Informe de análisis de riesgos • Informe emitido por los expertos con respecto a las políticas de seguridad existentes en la UPSE • Documento de políticas de seguridad revisadas y aprobadas • Actas de asistencia de los diversos grupos a la socialización	• Rector • Departamento de TIC´S	8 meses
Crear una política de control de accesos para las diversas áreas de la institución	• Solicitar al departamento administrativo un listado de las áreas que existen en la UPSE • Identificar las áreas críticas de la universidad con base a lo establecido de la norma ISO 27001 • Establecer la política de control de acceso a las áreas que contengan	• Informe de las áreas de la UPSE • Informe de las áreas críticas de la UPSE • Documento de políticas de control de acceso • Documento de políticas de seguridad de la UPSE	• Departamento de TIC´S • Departamento administrativo	2 meses

	información sensible • Solicitar incluir esta política en el documento actualizado de las políticas de seguridad de la institución	(verificar que exista la sección de control de acceso)		
Tema: Gestión de acceso de usuario			Subtema 1: Gestión de altas/bajas en el registro de usuarios	
Recomendación: Establecer un procedimiento formal de alta y baja de usuarios.				
Medidas sugeridas	**Acciones estratégicas**	**Indicadores**	**Responsables**	**Plazos**
Realizar un sistema de control de altas/bajas de usuarios que automatice el registro de estos	• Creación de un sistema de control con un módulo de altas/bajas de usuarios • Llevar un registro de estos eventos y oficializarlos a través de talento humano	• Implementación del módulo de altas/bajas de usuarios • Registro de altas/bajas de usuarios	• Departamento de TIC´S • Departamento de Talento Humano	4 meses
Tema: Gestión de acceso de usuario			Subtema 2: Gestión de los derechos de acceso asignados a usuarios	
Recomendación: Implantar un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios.				
Medidas sugeridas	**Acciones estratégicas**	**Indicadores**	**Responsables**	**Plazos**
Realizar un sistema de control de acceso a los usuarios que asigne o revoque los derechos de accesos a los sistemas y servicios de la universidad	• Creación de un sistema de control con un módulo de asignación o revocación de derechos de accesos a los sistemas y servicios de la UPSE • Llevar un registro de estos eventos y oficializarlos a través de talento humano	• Implementación del módulo de asignación o revocación de derechos de accesos • Registro de asignación o revocación de derechos de accesos a los usuarios	• Departamento de TIC´S • Departamento de Talento Humano	4 meses
Tema: Control de acceso a sistemas y aplicaciones			Subtema 1: Restricción del acceso a la información	
Recomendación: Restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, con relación a la política de control de accesos definida.				
Medidas sugeridas	**Acciones estratégicas**	**Indicadores**	**Responsables**	**Plazos**

Implementar las políticas de control de acceso	• Realizar un listado de personal autorizado en cada área y notificar • En las áreas altamente críticas hacer firmar un contrato de responsabilidad al personal involucrado sobre los activos • Seguir las recomendaciones establecidas en las políticas de seguridad de la UPSE	• Listado de personal autorizado por área • Contratos de responsabilidad • Documento de políticas de seguridad UPSE, sección control de acceso	• Departamento de TIC´S • Departamento de Talento Humano	3 meses
Tema: Control de acceso a sistemas y aplicaciones			Subtema 2: Uso de herramientas de administración de sistemas.	
Recomendación: Revisar en los equipos informáticos el uso de utilidades software que podrían ser capaces de anular o evitar controles en aplicaciones y sistemas para que se restrinja o controle su uso.				
Medidas sugeridas	**Acciones estratégicas**	**Indicadores**	**Responsables**	**Plazos**
Establecer de manera formal y documentada labores de mantenimiento programadas periódicamente para llevar un inventario actualizado de los equipos informáticos y sus softwares instalados	• Establecer a través de la dirección de TIC´S la realización del mantenimiento preventivo, correctivo y predictivo. • Realizar inventarios del software instalado en los equipos informáticos de la UPSE • Mantener actualizada las utilidades software necesarias de los equipos informáticos	• Informe de mantenimiento preventivo • Informe de mantenimiento correctivo • Informe de mantenimiento predictivo • Inventario del software instalado en cada máquina • Informe de la versión de las utilidades software instaladas en cada máquina	• Departamento de TIC´S	Se realizará por períodos. Dos veces en el año

Restringir la instalación de aplicaciones en los equipos informáticos conectados a la red de la UPSE	• Se limitará la descarga de software en los equipos informáticos conectados a la red de la UPSE • Se deberán configurar todas las computadores con el fin de restringir la instalación de software, sólo personal autorizado podrá realizarlo	• Firewall de control • Lista de usuarios con acceso	• Departamento de TIC´S	1 mes

Tabla 7: Plan de acción para el control de acceso

PLAN DE ACCIÓN: SEGURIDAD FÍSICA Y AMBIENTAL				
Tema: Áreas seguras			Subtema 1: Perímetro de seguridad física	
Recomendación: Definir y utilizar perímetros de seguridad, por ejemplo señaléticas, específicamente en las áreas o instalaciones de procesamiento de información sensible o crítica.				
Medidas sugeridas	**Acciones estratégicas**	**Indicadores**	**Responsables**	**Plazos**
Definir el nivel de seguridad de cada área de la UPSE de acuerdo con los activos que contienen	• Solicitar el listado de las áreas existentes en UPSE • Realizar una evaluación de cada área verificando los activos que posee y realizando un análisis de riesgo • Categorizar cada área de acuerdo con su nivel de impacto	• Listado de las áreas de la UPSE • Análisis de riesgo por área • Informe del nivel de impacto por área	• Departamento de TIC´S • Departamento Administrativo	4 meses
Instaurar señaléticas que permitan identificar los perímetros de seguridad de cada área	• Diseñar un bosquejo de perímetro en cada área para su aprobación • Implementar el diseño	• Bosquejo de perímetro revisado y aprobado • Informe de implementación del bosquejo	• Departamento de TIC´S	2 meses
Tema: Áreas seguras			Subtema 2: Controles físicos de entrada	
Recomendación: Implementar controles de entrada adecuados en las áreas de procesamiento de información crítica o sensible para garantizar que solo el personal autorizado dispone de permiso de acceso				
Medidas sugeridas	**Acciones estratégicas**	**Indicadores**	**Responsables**	**Plazos**
Implementar sistemas biométricos de control de acceso en las áreas de procesamiento de información crítica o sensible	• Adquirir sistemas biométricos para el control de acceso en las áreas denominadas como “áreas críticas” • Instalar los sistemas biométricos en las áreas	• Sistema biométrico instalados en las áreas	• Departamento de TIC´S	3 meses
Tema: Áreas seguras			Subtema 3: Seguridad de oficinas,	

			despachos y recursos	
Recomendación: Diseñar y aplicar un sistema de seguridad física a las oficinas, salas e instalaciones de la organización basados en un análisis de riesgo.				
Medidas sugeridas	**Acciones estratégicas**	**Indicadores**	**Responsables**	**Plazos**
Reubicar los equipos de las oficinas con el fin de minimizar riesgos y que se sitúen con espacios requeridos en la norma ISO 27002	• Identificar la ubicación de los equipos y verificar que se encuentren en el margen establecido por la ISO 27002 • Verificar el estado del cableado de red y eléctrico	• Informe de ubicación de equipos • Inventarios de equipos	• Departamento de TIC´S	2 meses
Proveer protección física a los equipos informáticos	• Adquirir materiales que brinden seguridad física a los equipos de cómputo, tales como, reguladores, supresor de picos, UPS, forros protectores para computadoras de escritorio, mica protectora de pantalla, etc.	• Informe de instalación de equipos de protección física	• Departamento de TIC´S	2 meses
Tema: Seguridad de los equipos			Subtema 1: Emplazamiento y protección de equipos	
Recomendación: Realizar un control formal de la entrada/salida de los equipos				
Medidas sugeridas	**Acciones estratégicas**	**Indicadores**	**Responsables**	**Plazos**
Implementar un sistema de control para el registro de entrada/salida de los equipos de cada área	• Receptar las solicitudes de entrada/salida de equipos • Crear un sistema de control con un módulo para registrar la entrada/salida de equipos informáticos • Registrar el estado, serie, funcionalidad, área perteneciente, entre otros del equipo • Firmar actas de entrega y	• Registro de entrada/salida de equipos • Actas de entrega y responsabilidad	• Departamento de TIC´S • Departamento de activo fijo • Responsable del área perteneciente al equipo	4 meses

	responsabilidad			
Tema: Seguridad de los equipos			Subtema 2: Equipo informático de usuario desatendido.	
Recomendación: Realizar un inventario de inspección periódica a los equipos no supervisados conectados a la red de la institución.				
Medidas sugeridas	**Acciones estratégicas**	**Indicadores**	**Responsables**	**Plazos**
Todos equipos conectados a la red deben estar autorizados y registrados para su respectivo control	• Restringir la conexión a la red de la UPSE a los equipos que no se encuentren registrados • Realizar una revisión periódica en el firewall de control para verificar el estado del tráfico de la red de los dispositivos	• Informe del firewall con respecto al tráfico en la red	• Departamento de TIC´S	3 meses

Tabla 8: Plan de acción para la seguridad física y ambiental

CONCLUSIONES

- La recopilación de información que se realizó en el departamento de TIC´s fue fundamental para realizar el presente trabajo investigativo, este proceso permitió verificar que esta dependencia carece de documentos esenciales tales como: el análisis de riesgo, políticas de control de acceso, perimetrización en áreas críticas, etc. Además cabe indicar que existen procesos que se ejecutan, sin embargo, no se encuentran en documentación formalizada como por ejemplo los mantenimientos preventivos, correctivos y predictivos, alta/baja de usuarios, etc.
- La norma 27002 se basa en las buenas prácticas que se deben implementar en un sistema de gestión de información, por ende, el baremo aplicado se constituyó en un instrumento fundamental para constatar el estado actual del departamento, tanto en su control de acceso como en la seguridad física y ambiental de los equipos. El informe de resultados del baremo plasmó las observaciones de acciones correctivas que debe de considerar el departamento de TIC´s considerando que esta unidad administrativa es el eje central y custodio del activo más importante de la institución que es la información.
- El diseño del plan de acción tanto para el control de acceso como para la seguridad física y ambiental de los equipos se adapta a las necesidades actuales de la UPSE y mitigará los posibles riesgos que determinó este trabajo investigativo a través de las técnicas de recolección de datos basados en el proceso metodológico. El plan de acción propuesto presenta las estrategias e indicadores necesarios que permitirán a las autoridades pertinentes tomar decisiones y establecer acciones con la respectiva temporalidad.

RECOMENDACIONES

- Fundamentándose en la información presentada en esta investigación se recomienda al gestor del departamento de TIC´S que coordine acciones a la brevedad posible para realizar un análisis de riesgo, debido a que, este análisis será el insumo principal para poder implementar el plan de acción.
- Las políticas de seguridad que actualmente están vigentes y aprobadas en la UPSE se basaron en la norma ISO 27002 que es un referente internacional, sin embargo, se consideran políticas muy generalizadas e incompletas, por ende, se sugiere que se creen nuevas políticas que complementen las existentes y además se alineen a los objetivos institucionales de la UPSE
- El presente trabajo investigativo se basó específicamente en la sección 9 y 11 de la norma ISO 27002, prospectivamente, se recomienda que en futuras investigaciones se consideren las demás secciones y así poderlas integrar en el plan de acción propuesto.

BIBLIOGRAFÍA

[1] G. Disterer, «ISO/IEC 27000, 27001 and 27002 for Information Security Management,» *Scientific Research,* vol. 4, nº 2, pp. 92-100, 2013.

[2] A. Calder, Implementing Information Security based on ISO 27001/ISO 27002, Van Haren, 2011.

[3] Ostec, «ISO 27002: Buenas prácticas para gestión de la seguridad de la información,» Ostec, 2016 Diciembre 30. [En línea]. Available: https://ostec.blog/es/aprendizaje-descubrimiento/iso-27002-buenas-practicas-gsi/. [Último acceso: 2023 Abril 18].

[4] ISO 27000, «ISO 27000,» 2005. [En línea]. Available: https://www.iso27000.es/iso27002.html. [Último acceso: 2023 Abril 19].

[5] UPSE, «Estructura orgánica funcional de la Universidad Estatal Península de Santa,» UPSE, La Libertad, 2014.

[6] UPSE, «Manual de políticas de seguridad de la UPSE,» UPSE, La Libertad, 2018.

[7] J. Jara Arenas, «Framework de seguridad de la información basado en los controles de la ISO 27002 para el proceso académico de la UNT,» Repositorio Digital de la Universidad Privada Antenor Orrego, 2019.

[8] M. F. Meigs y A. T. Jersild, «Chapter V: Direct Observation as a Research Method,» *Review of Educational Research,* vol. 9, nº 5, pp. 472-482, 1939.

[9] C. Martinez, «Observación directa: características, tipos y ejemplo,» 2021. [En línea]. Available: https://www.lifeder.com/observacion-directa/. [Último acceso: 2023 Abril 20].

[10] J. A. Grados Espinosa y E. Sánchez Fernández, La entrevista en las organizaciones, México: Editorial El Manual Moderno, 2017.

[11] L. Díaz-Bravo, U. Torruco-García y M. Martínez-Hernández, «La entrevista, recurso flexible y dinámico,» *Investigación en Educación Médica,* vol. 2, nº 7, pp. 162-167, 2013.

[12] Secretaria General de Planificación, «Plan de Creación de Oportunidades 2021-2025,» 2021. [En línea]. Available: https://observatorioplanificacion.cepal.org/sites/default/files/plan/files/Plan-de-Creaci%C3%B3n-de-Oportunidades-2021-2025-Aprobado_compressed.pdf. [Último acceso: 2023 Abril 27].

[13] F. J. Valencia-Duque y M. Orozco-Alzate, «Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000,» *RISTI,* nº 22, pp. 73-88, 2017.

[14] J. E. Garcia Rivera y C. A. Del Águila Salas, Análisis e implementación de la seguridad de la información del centro de datos de la Universidad Nacional de la Amazonía Peruana bajo la norma ISO 27002, Iquitos: Universidad Nacional de la Amazonía Peruana, 2017.

[15] D. Romo Villafuerte y J. Valarezo Constante, «Análisis e Implementación de la Norma ISO 27002 para el Departamento de Sistemas de la Universidad Politécnica Salesiana Sede Guayaquil,» Repositorio Institucional de la Universidad Politécnica Salesiana, Guayaquil, 2012.

[16] C. A. Avenía Delgado, Fundamentos de seguridad informática, Bogotá: Fundación Universitaria del Área Andina, 2017.

[17] J. Costas Santos, Seguridad informática, Ra-Ma Editorial, 2010.

[18] E. Vega Briceño, Seguridad de la información, 3Ciencias, 2021.

[19] L. Guallpa Zatán, plan de seguridad informática basada en la norma ISO 27002 para el control de accesos indebidos a la red de UNIANDES Puyo, Ambato: UNIANDES, 2017.

[20] C. E. Barrantes Porras y J. R. Hugo Herrera, Diseño e implementación de un Sistema de Gestión de Seguridad de Información en procesos tecnológicos, Universidad de San Martín de Porres, 2008.

[21] J. G. Arévalo Ascanio, R. A. Bayona Trillos y D. W. Rico Bautista, «Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información,» *Tecnura,* vol. 19, nº 46, pp. 123-134, 2015.

[22] A. C. Nieves, Diseño de un sistema de gestión de la seguridad de la información (SGSI) basados en la norma Iso/iec 27001:2013, Politecnico Grancolombiano, 2013.

[23] Á. Y. Ducuara Cruz y J. A. Moya Molano, Manual de buenas prácticas sobre la seguridad de la información sensible de la entidad del DANE, Bogota: Politécnico Grancolombiano, 2017.

[24] V. A. Fontalvo Ardila, Conceptos básicos en buenas practicas en gestión de TI y seguridad de la información, 2017.

[25] ISO, ONUDI, Organismos Nacionales de Normalización en Países en Desarrollo, Ginebra: Secretaría Central de la ISO.

[26] ISO Tools, «ISO Tools,» Grupo ESGinnova, [En línea]. Available: https://www.isotools.us/normas/. [Último acceso: 1 05 2023].

[27] A. Calder y S. Watkins, Information Security Risk Management for ISO27001/ISO27002, United Kingdom: IT Governance Ltd, 2010.

[28] ALTAOS, «ISO 27002,» ALTAOS, 2017. [En línea]. Available: https://www.leydeprotecciondatospersonales.com/iso_27002/#:~:text=La%20ISO%2027002%20contiene%20un,en%20todos%20los%20%C3%A1mbitos%20posibles. [Último acceso: 29 04 2023].

[29] M. Naghi Namakforoosh, Metodología de la investigación, Editorial Limusa, 2000.

[30] S. Galeana De La O, Promoción social una opción metodológica, México: Plaza y Valdés, 1999.

[31] ISO27000, «ISO27000.es: Anexo 9,» ISO27000, 2005. [En línea]. Available: https://www.iso27000.es/iso27002_9.html. [Último acceso: 23 6 2023].

[32] ISO27000, «ISO27000.es: Anexo 11,» ISO27000, 2005. [En línea]. Available: https://www.iso27000.es/iso27002_11.html#:~:text=Los%20medios%20de%20procesamiento%20de%20informaci%C3%B3n%20cr%C3%ADtica%20o,protegidos%20del%20acceso%20no%20autorizado,%20da%C3%B1o%20e%20interferencia.. [Último acceso: 23 6 2023].

[33] M. Sáenz Casallas, Elaboración de un plan de implementación de la ISO/IEC 27001:2013 para una ISP, Cali: Universitat Oberta de Catalunya (UOC), 2020.

[34] Y. A. Cornejo Montoya, Desarrollo e implementación de control para el dominio de seguridad física y ambiental para la empresa FELMOVA S.A. usando la norma ISO 27002:2013, Guayaquil: Escuela Superior Politécnica del Litoral, 2017.

ANEXOS

ANEXO 1: Guion de entrevista

Objetivo: Obtener información a través de preguntas abiertas dirigidas al director del departamento de TIC´S respecto al tratamiento de la información en la UPSE para el proyecto de investigación "implementación de un plan de acción para las buenas prácticas en la gestión de la seguridad de la información del departamento de TIC´s de la UPSE"	
Datos de identificación de la entrevista:	
Día de la entrevista: Tiempo estimado de entrevista (presencial): Hora de la entrevista: Locación donde se realizó la entrevista:	 60 minutos Dirección de departamento de TIC´S
Datos de identificación de la persona entrevistada:	
Nombre: Profesión Cargo:	Fabricio Ramos Ing. En Sistemas – Magister Director de TIC´S

Preguntas:

1. ¿Cuántas áreas tiene el departamento de TIC´S y qué funciones tiene cada una?

2. ¿La UPSE tiene establecido sus políticas de seguridad?

3. ¿Hace cuánto tiempo fueron creadas estas políticas?

4. ¿Considera usted que las políticas de seguridad de la UPSE son óptimas para la protección de la información de la organización?

5. ¿Cuál es el plan de acción que tiene el departamento de TIC´S para la prevención, mitigación y atención de riesgos?

6. ¿Cuál es la metodología que utilizan ustedes para el análisis de riesgo?

7. ¿Cuándo fue el último análisis de riesgo que realizó el departamento?

8. ¿Cuál es la metodología que utilizan ustedes para el análisis de riesgo?

9. ¿Cuándo fue el último análisis de riesgo que realizó el departamento?
10. ¿En qué documento se encuentran plasmadas las reglas y normas para el control de acceso en áreas críticas como el área de desarrollo de software, área de servidores, etc.?

11. ¿Cómo han sido socializadas estas reglas de control a los entes internos (personal que trabaja en TIC´S) y externos del departamento (docentes, estudiantes, administrativos?

12. ¿Cuáles son las técnicas que ustedes utilizan para dar seguridad en el procesamiento de la información? (por ejemplo: tipo de encriptación, seguridad en redes, etc.)

13. ¿Basados en qué regularización crearon la estructura física de cada área del departamento, especialmente el data center?

14. ¿Cómo se concatenan las políticas de seguridad actuales con los objetivos institucionales?

15. ¿Considera útil la creación de un plan de acción para las buenas prácticas en el SGSI? ¿Por qué?

ANEXO 2: Baremo del control de acceso ISO 27002

9. CONTROL DE ACCESOS.						
9.1 Requisitos de negocio para el control de accesos.						
Control	**Descripción**	**Métrica**	**SI**	**NO**	**TALVEZ**	**OBSERVACIONES**
9.1.1 Política de control de accesos.	Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.	Porcentaje de sistemas y aplicaciones corporativas para los que los "propietarios" adecuados han: (a) sido identificados, (b) aceptado formalmente sus responsabilidades, (c) llevado a cabo -o encargado- revisiones de accesos y seguridad de aplicaciones, basadas en riesgo y (d) definido las reglas de control de acceso basadas en roles.				
9.1.2 Control de acceso a las redes y servicios asociados.	Se debería proveer a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar.					
9.2 Gestión de acceso de usuario.						
Control	**Descripción**	**Métrica**	**SI**	**NO**	**TALVEZ**	**OBSERVACIONES**
9.2.1 Gestión de altas/bajas en el registro de usuarios.	Debería existir un procedimiento formal de alta y baja de usuarios con objeto de habilitar la asignación de derechos de acceso.	Tiempo medio transcurrido entre la solicitud y la realización de peticiones de cambio de accesos y número de solicitudes de cambio de acceso cursadas en el mes anterior (con análisis de tendencias y comentarios acerca de cualquier pico / valle (p. ej., "Implantada				
9.2.2 Gestión de los derechos de acceso	Se debería de implantar un proceso formal de aprovisionamiento de					

asignados a usuarios.	accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios.	nueva aplicación financiera este mes").				
9.2.3 Gestión de los derechos de acceso con privilegios especiales.	La asignación y uso de derechos de acceso con privilegios especiales debería ser restringido y controlado.					
9.2.4 Gestión de información confidencial de autenticación de usuarios.	La asignación de información confidencial para la autenticación debería ser controlada mediante un proceso de gestión controlado.					
9.2.5 Revisión de los derechos de acceso de los usuarios.	Los propietarios de los activos deberían revisar con regularidad los derechos de acceso de los usuarios.					
9.2.6 Retirada o adaptación de los derechos de acceso	Se deberían retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo,					

	contrato o acuerdo, o ser revisados en caso de cambio.					
9.3 Responsabilidades del usuario.						
Control	**Descripción**	**Métrica**	**SI**	**NO**	**TALVEZ**	**OBSERVACIONES**
9.3.1 Uso de información confidencial para la autenticación.	Se debería exigir a los usuarios el uso de las buenas prácticas de seguridad de la organización en el uso de información confidencial para la autenticación.	Porcentaje de descripciones de puesto de trabajo que incluyen responsabilidades en seguridad de la información (a) totalmente documentadas y (b) formalmente aceptadas.				
9.4 Control de acceso a sistemas y aplicaciones.						
Control	**Descripción**	**Métrica**	**SI**	**NO**	**TALVEZ**	**OBSERVACIONES**
9.4.1 Restricción del acceso a la información.	Se debería restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación con la política de control de accesos definida.	Porcentaje de soportes de backup o archivo que están totalmente encriptados.				
9.4.2 Procedimientos seguros de inicio de sesión.	Cuando sea requerido por la política de control de accesos se debería controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de log-on					

9.4.3 Gestión de contraseñas de usuario.	Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar contraseñas de calidad.					
9.4.4 Uso de herramientas de administración de sistemas.	El uso de utilidades software que podrían ser capaces de anular o evitar controles en aplicaciones y sistemas deberían estar restringidos y estrechamente controlados.					
9.4.5 Control de acceso al código fuente de los programas.	Se debería restringir el acceso al código fuente de las aplicaciones software.					

ANEXO 3: Baremo de la seguridad física y ambiental ISO 27002

11. SEGURIDAD FÍSICA Y AMBIENTAL.						
11.1 Áreas seguras.						
Control	**Descripción**	**Métrica**	**SI**	**NO**	**TALVEZ**	**OBSERVACIONES**
11.1.1 Perímetro de seguridad física.	Se deberían definir y utilizar perímetros de seguridad para la protección de las áreas que contienen información y las instalaciones de procesamiento de información sensible o crítica.	Informes de inspecciones periódicas de seguridad física de instalaciones, incluyendo actualización regular del estado de medidas correctivas identificadas en inspecciones previas que aún estén pendientes.				
11.1.2 Controles físicos de entrada.	Las áreas seguras deberían estar protegidas mediante controles de entrada adecuados para garantizar que solo el personal autorizado dispone de permiso de acceso.					
11.1.3 Seguridad de oficinas, despachos y recursos.	Se debería diseñar y aplicar un sistema de seguridad física a las oficinas, salas e instalaciones de la organización.					
11.1.4 Protección contra las amenazas externas y ambientales.	Se debería diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes.					

11.1.5 El trabajo en áreas seguras.	Se deberían diseñar y aplicar procedimientos para el desarrollo de trabajos y actividades en áreas seguras.					
11.1.6 Áreas de acceso público, carga y descarga.	Se deberían controlar puntos de acceso a la organización como las áreas de entrega y carga/descarga (entre otros) para evitar el ingreso de personas no autorizadas a las dependencias aislando estos puntos, en la medida de lo posible, de las instalaciones de procesamiento de información.					
11.2 Seguridad de los equipos						
Control	**Descripción**	**Métrica**	**SI**	**NO**	**TALVEZ**	**OBSERVACIONES**
11.2.1 Emplazamiento y protección de equipos.	Los equipos se deberían emplazar y proteger para reducir los riesgos de las amenazas y peligros ambientales y de oportunidades de acceso no autorizado.	Número de chequeos (a personas a la salida y a existencias en stock) realizados en el último mes y porcentaje de chequeos que evidenciaron movimientos no autorizados de equipos o soportes informáticos u otras cuestiones de seguridad.				
11.2.2 Instalaciones de suministro.	Los equipos deberían estar protegidos contra cortes de luz y otras interrupciones					

	provocadas por fallas en los suministros básicos de apoyo.					
11.2.3 Seguridad del cableado.	Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se deberían proteger contra la intercepción, interferencia o posibles daños.					
11.2.4 Mantenimiento de los equipos.	Los equipos deberían mantenerse adecuadamente con el objeto de garantizar su disponibilidad e integridad continuas.					
11.2.5 Salida de activos fuera de las dependencias de la empresa.	Los equipos, la información o el software no se deberían retirar del sitio sin previa autorización					
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	Se debería aplicar la seguridad a los activos requeridos para actividades fuera de las dependencias de la organización y en consideración de los distintos riesgos.					
11.2.7 Reutilización o retirada segura	Se deberían verificar todos los equipos que contengan medios de almacenamiento					

de dispositivos de almacenamiento.	para garantizar que cualquier tipo de datos sensibles y software con licencia se hayan extraído o se hayan sobrescrito de manera segura antes de su eliminación o reutilización.					
11.2.8 Equipo informático de usuario desatendido.	Los usuarios se deberían asegurar de que los equipos no supervisados cuentan con la protección adecuada.	Informes de inspecciones periódicas a los equipos, incluyendo actividades para la revisión de rendimiento, capacidad, eventos de seguridad y limpieza de los diversos componentes (aplicaciones, almacenamiento, CPU, memoria, red, etc.).				
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla	Se debería adoptar una política de puesto de trabajo despejado para documentación en papel y para medios de almacenamiento extraíbles y una política de monitores sin información para las instalaciones de procesamiento de información.					