INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

TEMA DE INVESTIGACIÓN:

ANÁLISIS DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA PUCE-E BASADO EN LA NORMA ISO 27001

TESIS DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

AUTOR:

DENYS DANIELA ANGULO CHICA

ASESOR:

MGT. HOMERO VELASTEGUÍ

ESMERALDAS, 2024

TRIBUNAL DE GRADUACIÓN

Título: Análisis de un sistema de gestión de seguridad de la información para la PUCE-E basado en la norma ISO 27001.

Autor(a): Denys Daniela Angulo Chica

Mgt. Homero Velasteguí
Asesor
f._____

Mgt. José Luis Carvajal
Lector #1
f._____

Mgt. Xavier Quiñonez
Lector #2
f._____

Mgt. Homero Velasteguí
Coordinadora de Carrera
f._____

AUTORÍA

Yo, **Denys Daniela Angulo Chica** con número de cédula de identidad 0850272048 manifiesto que mediante la presente investigación sobre el tema "**ANALISIS DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA PUCE-E BASADO EN LA NORMA ISO 27001**" los resultados obtenidos como tesis de grado, previo a la obtención del título de "**INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN**" son de total responsabilidad del autor, y que se ha respetado las fuentes de información consultadas, realizando las citas correspondientes y los resultados alcanzados son totalmente personales, únicos y legítimos. A la vez, declaro que el contenido incluyendo resultados, discusión, conclusiones, recomendaciones y otros efectos legales y académicos que se desglosan son y serán responsabilidad legal y académica del autor y de la PUCE-E.

_____

Denys Daniela Angulo Chica
C.I 0850300948

AGRADECIMIENTOS

Le agradezco a Dios por ser refugio y fortaleza en mi vida, llenándome de bendiciones cada día, por darme la sabiduría y salud para poder obtener este logro.

Agradezco a mi madre por motivarme, aconsejarme, apoyarme y formarme en cada paso de este proceso, siendo mi pilar fundamental terrenalmente.

Como no agradecer a mis profesores, que han visto mi desarrollo y crecimiento a lo largo de mi carrera, quienes me han brindado de su conocimiento, dedicación, consideración. A mi asesor, Mgt. Homero Velastegui por brindarme sus conocimientos, tiempo e interés a lo largo de este trayecto.

Finalmente, agradezco al amor de mi vida Fernando, que ha estado conmigo siempre, apoyándome y aconsejándome en todo momento; a los amigos y compañeros que me ha dado la Universidad, Lisseth, Pablo, Santiago y Brayan, que llegaron a mi vida para llenarme de alegrías, gracias por la amistad brindada y los buenos momentos en este proceso académico.

DEDICATORIA

Dedico este trabajo a Dios, por darme salud, fuerza y sabiduría para cumplir con esta meta en mi vida y no dejarme decaer a lo largo de este proceso.

Dedico con todo mi corazón a mi madre Angela Chica, por ser el pilar fundamental para que yo haya conseguido este logro, por siempre motivarme y apoyarme en cada paso que doy en mi vida, sobre todo por ser una mujer luchadora y trabajadora, siendo mi ejemplo y orgullo para seguir cumpliendo muchas metas más.

RESUMEN

El objetivo del presente estudio es analizar un sistema de gestión de seguridad de la información para la PUCE-E basándose en la norma ISO 27001 con el propósito de mejorar la administración integral de los activos de información. Para llevar a cabo esta investigación fue necesario elaborar un inventario de activos en el cual se consideró estudios publicados del periodo 2018- 2021. El estudio fue desarrollado a partir de una metodología descriptiva, cualitativa y cuantitativa como técnica principal se realizó una entrevista y como instrumento se utilizó una tabla, donde se detallaron todos los activos con sus respectivas características y se evaluó el nivel de impacto de cada uno utilizando los tres pilares de la seguridad de la información que son confidencialidad, integridad y disponibilidad. El análisis de los datos permitió conocer cuáles son los activos que tendrían un mayor impacto, cuáles son los activos donde hay más datos sensibles o personales y quien es el propietario con más activos a su cargo. Se concluyo que los activos de información de la PUCE-E, tienen un nivel de impacto alto que podría tener repercusiones económicas en caso de ser vulnerados, esto demostró la importancia de implementar un sistema de gestión de seguridad de la información.

Palabras clave: ISO 27001, ISO 27002, activos, seguridad de la información.

Abstract

The objective of this study is to analyze an information security management system for PUCE-E based on the ISO 27001 standard in order to improve the comprehensive management of information assets. To carry out this research, it was necessary to prepare an asset inventory in which published studies from the 2018-2021 period were considered. The study was developed from a descriptive, qualitative and quantitative methodology. An interview was conducted as the main technique and a table was used as an instrument, where all the assets were detailed with their respective characteristics and the level of impact of each one was evaluated using the three pillars of information security which are confidentiality, integrity and availability. The analysis of the data made it possible to know which assets would have the greatest impact, which are the assets where there is more sensitive or personal data and who is the owner with the most assets under their charge. It was concluded that the information assets of PUCE-E have a high level of impact that could have economic repercussions if they are breached, which demonstrated the importance of implementing an information security management system.

Keywords: ISO 27001, ISO 27002, assets, information security.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Presentación del problema

La seguridad de la información es relevante para una empresa privada por la confidencialidad que debe mantener, a medida que pasa el tiempo se busca la forma adecuada para detectar las posibles amenazas y para crear un sistema que funcione como una barrera ante las vulnerabilidades.

Muchas empresas en todo el mundo optan por utilizar normas internacionales, como la familia de las ISO 27000, debido a la necesidad de emplear un sistema de gestión de riesgos funcional y certificado [1]. La norma ISO 27001, es un reglamento estandarizado que es utilizado a nivel internacional de referencia para evaluar la gestión y los riesgos de las empresas, aplicable a los proveedores del servicio, independientemente de su tipo, tamaño o naturaleza de los servicios entregados [2].

El diseño e implementación de un sistema de gestión de seguridad de la información empleando las normas ISO 27001, puede controlar las amenazas, vulnerabilidades y los riesgos de seguridad a que se ve expuesta una empresa [3]. Cuando se analiza la vulnerabilidad de cada activo, se puede elaborar un plan de gestión de riesgos, considerando los controles implementados en la empresa para luego implementar otras herramientas o procesos que disminuyan los riesgos.

La información dependiendo de su grado de confidencialidad puede ser el activo más valioso de una empresa [4], comprobar la eficacia de la empresa para salvaguardar datos sensibles contribuye a su prestigio e imagen, tener un sistema avalado que le asegure a los clientes y miembros de la empresa que sus datos estarán seguros, consolida la confianza de estas personas provocando que deseen seguir obteniendo y prestando sus servicios; a su vez también ocasiona que las personas externas deseen ser parte de una empresa que cuenta con prestigio y garantías de seguridad.

Los activos de una empresa pueden tener varios riesgos, a medida que avanza la tecnología los riesgos incrementan, así como hay avances tecnológicos también hay mejoras para los softwares especializados en vulnerar la información, las personas mal intencionadas crean nuevos procesos para atacar la seguridad.

Planteamiento del problema

Existen muchos factores que pueden suponer un riesgo o una vulnerabilidad, se han desarrollado varias herramientas y normas que pueden controlarlas para garantizar la seguridad de la información. Se podrá demostrar cómo el uso de las normas ISO 27001 y todo el proceso que conlleva emplearlas disminuye considerablemente los riesgos de los activos de la empresa que tengan una vulnerabilidad mayor [5].

Es un hecho que la importancia de la seguridad de la información es un tema técnico que también involucra a los procesos de negocio, como lo son la confianza entre la empresa y los clientes e incluso entre los mismos miembros de la empresa; las actividades de gobierno corporativo forman parte de la seguridad de la información que garantiza la constante evaluación de los riesgos a su vez afianzan que se mantendrá la seguridad de los activos requerida por la empresa [3].

Un gran problema que se da en las empresas a la hora de hacer una declaración de aplicabilidad son los factores externos y las relaciones interpersonales, es por esto que lo indicado es que la auditoría sea realizada por un profesional externo a la empresa y en caso de que la persona que realizará el proceso pertenezca a la empresa o tenga alguna relación personal con los miembros de la empresa [6], el auditor deberá mantener una actitud profesional basada en los principios de auditoría de las normas ISO 27000 garantizando la ética con la que se hará el proceso y la veracidad de la información que se presentará.

Aplicar un sistema de gestión de seguridad de la información no solo protege a la información de una empresa como activo, al mitigar los riesgos evita pérdidas financieras en caso de vulneración de la información y dándole otro enfoque en el ámbito legal aplicando las normas ISO 27001 favorece que las empresas puedan acatar los requerimientos legales de las entidades de control [7].

En esta investigación se ha decidido hacer un análisis de un sistema de gestión de seguridad de la información para la PUCE-E basado en la norma ISO 27001. Sin embargo, previo a realizar el análisis se requiere responder a las siguientes preguntas. (i) ¿Cuáles son los activos de información de los procesos o áreas críticas de la PUCE-E?, (ii) ¿Qué activos se evaluarán mediante las dimensiones de seguridad de la información?,

(iii) ¿Cuál será el resultado de la declaración de aplicabilidad mediante los lineamientos de la norma ISO/IEC 27001?

Justificación

El cibercrimen es un problema creciente para la educación superior, al igual que otras industrias, el sector educativo también está experimentando un aumento espectacular de los ataques de cibernéticos. Muchas universidades han experimentado un intento de ataque, con resultados que van desde la interrupción limitada del servicio hasta la filtración de datos, esta investigación tiene la intención de elaborar un análisis de un sistema de gestión de seguridad de la información para Pontificia Universidad Católica del Ecuador Sede Esmeraldas (PUCE-E) con la finalidad de distinguir cuales son los activos que se emplean en los procesos o áreas críticas y evaluar cual sería el nivel de impacto al ser vulnerados.

Un motivo fundamental por el cual se realiza este estudio es para redactar una declaración de aplicabilidad usando la norma internacional ISO 27001, que permita identificar qué controles se han implementado y cuáles son los aspectos que no se han tomado en cuenta para garantizar la seguridad de la información en los procesos.

La PUCE-E es una institución prestigiosa que ofrece una formación académica, debe obtener la información de sus usuarios para realizar varios procesos, estos datos deben ser almacenados de forma segura. Un sistema de gestión de seguridad de la información sería una herramienta muy útil, en esta investigación se analizarán los beneficios que podría tener para los departamentos claves.

Por lo tanto, es importante identificar las áreas vulnerables que puedan afectar a los procesos realizados en los departamentos, para así en base a estos planear cual es la mejor forma de mitigar los riesgos. Además, este estudio es relevante porque se basa en la norma ISO 27001 que garantizará la seguridad e integridad de los procesos de la universidad.

Objetivos:

General

Analizar un sistema de gestión de seguridad de la información para la PUCE-E basándose en la norma ISO 27001 con el propósito de mejorar la administración integral de los activos de información.

Específicos

a) Identificar los activos de información de los procesos o áreas críticas de la PUCE-E mediante la aplicación de los lineamientos propuestos en la norma ISO/IEC 27002.
b) Evaluar el impacto de los activos, utilizando las dimensiones de seguridad de la información, para comprender su relevancia y criticidad en el contexto del sistema de gestión.
c) Realizar una declaración de aplicabilidad, mediante los lineamientos de la norma ISO/IEC 27001 para la PUCE-E, con el fin de proporcionar una guía específica para la implementación de medidas de seguridad.

CAPÍTULO I: MARCO TEÓRICO

1.1. Bases teóricas científicas

1.1.1 Seguridad de la información

La seguridad de la información es invaluable para las empresas, respalda la confidencialidad, disponibilidad e integridad; esto involucra la aplicación y gestión de controles. Sin embargo, la información también es vulnerable a las amenazas. Los ciberataques, la pérdida de datos y los errores humanos pueden provocar incidentes de seguridad que pueden provocar pérdida de datos, interrupción del negocio y daños a la reputación [8].

La seguridad de la información se logra estableciendo procesos y controles, que deben se aplicados por medio de un proceso de gestión de riesgos mediante un SGSI (Sistema de Gestión de Seguridad de la Información), que es un plan documentado para gestionar la seguridad relacionada con la tecnología de su organización. Esto incluye documentar los riesgos y tomar medidas para gestionarlos. El objetivo es proteger los datos de su empresa y evitar violaciones de seguridad. Las organizaciones deben realizar evaluaciones de riesgos continuas para identificar riesgos y vulnerabilidades de seguridad. Las empresas deben tomar medidas de protección mediante el despliegue de un equipo de TI para monitorear estos riesgos.

La seguridad de la información se rige por tres pilares de los aspectos de seguridad de la información que son confidencialidad, integridad y disponibilidad que se puede apreciar en la Figura 1. La confidencialidad es un aspecto que asegura que a la información solo podrán acceder personas autorizadas. La integridad es un aspecto que proporciona que los datos no se cambian o modifican sin permiso de las partes autorizadas. La disponibilidad es un aspecto que asegura que los datos estarán disponibles cuando sea necesario [9].

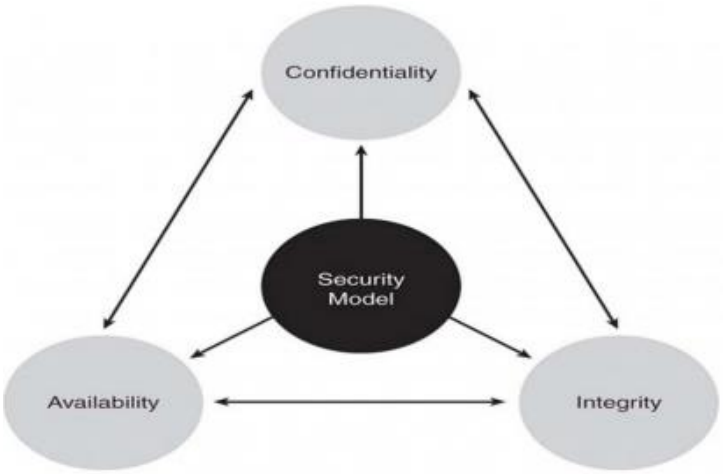

Figura 1. Modelo de seguridad de TI CIA [10].

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

ISO 27001 define SGSI como "un sistema de gestión que lleva a cabo el establecimiento, operación, mantenimiento, monitoreo y continuo de la seguridad de la información" [2]. El objetivo del SGSI es reducir el riesgo y garantizar la continuidad del negocio mediante restringir de forma proactiva el impacto de una infracción de seguridad [11].

Un SGSI es un conjunto de procedimientos y reglas dentro de una organización que sirven para identificar riesgos, definir, controlar, controlar, mantener, mejorar continuamente los requisitos específicos de la organización y los objetivos de protección en materia de seguridad de la información, sobre todo el desarrollo de la organización y su adaptarse periódicamente a las influencias externas. Básicamente, se trata de un enfoque basado en el riesgo y orientado al proceso con una mejora continua del nivel de protección [8].

También se puede definir un SGSI como un sistema compuesto por procesos, tecnologías y personas con el objetivo de administrar, monitorear, auditar y mejorar la seguridad de la información en una empresa [9].

La implementación del SGSI incluye recursos humanos, políticas, procedimientos y también software y hardware como parte de tecnología. Al implementar SGSI, puede dar a la organización la protección de la información contra diversos tipos de riesgos en la seguridad de la información. Como parte del SGSI está la gestión de riesgos, que es el proceso de identificar y evaluar el riesgo y tomar medidas para reducir el riesgo a un nivel aceptable. La evaluación de riesgos debe identificar riesgos y vulnerabilidades

potenciales con respecto a la confidencialidad, integridad y disponibilidad. Ayudará organización para reconocer y dar el control apropiado para reducir y gestionar el riesgo adecuadamente entre personas, procesos y tecnología.

Al llevar a cabo la implementación de un SGSI incluye recursos humanos, políticas, métodos y además programa y hardware como parte de tecnología. Al implementar un SGSI, puede ofrecer a la organización la seguridad de la información contra diferentes tipos de amenazas que puedan afectar a la información. Como parte del SGSI está la gestión de riesgos, que es el proceso de detectar y evaluar las vulnerabilidades y tomar medidas para degradarlas a un grado aceptable. La evaluación de riesgos debería detectar amenazas y vulnerabilidades potenciales con relación a la confidencialidad, integridad y disponibilidad; ayudará a la organización para reconocer y ofrecer el control apropiado para mitigar y gestionar el peligro correctamente entre gente, procesos y tecnología [9].

1.1.3 Familia de normas ISO 27000

La familia de normas ISO / IEC 27000 consta de un vocabulario estándar, tres estándares de requisitos, once pautas o normas, seis normas de directriz específicas del sector y tres normas de directriz específicas de control [11]. En un mundo donde la seguridad de la información de cualquier empresa es importante, la familia de las normas ISO 27000 es una opción ideal por todas las características que posee para diseñar un Sistema de Gestión de la Seguridad de la Información.

Por ejemplo, ISO 27002 es una guía de prácticas sobre sistema de gestión de seguridad de la información (SGSI) implementación, es un estándar que se complementa con ISO 27001. ISO 27002 antes conocida como ISO 17799, fue elaborada partiendo de BS 7799 Parte 1. La norma ISO 27005 detalla el proceso adecuado para la gestión de riesgos de seguridad de la información, enfocándose en la gestión de riesgos acogida por ISO 27001 [2]. Es importante conocer la relación entre los integrantes de la familia de las ISO 27000, ya que cada norma puede usarse en diferentes fases del proceso para implementar un SGSI. Para analizar una propuesta usando la ISO 27001, se debe tener en cuenta el proceso completo con el apoyo con las demás normas.

Las relaciones entre la familia de estándares SGSI como se detalla en la Figura 2 se divide en normas que especifican requisitos, hay algunos estándares que describen pautas generales y hay otros que describen las pautas específicas.

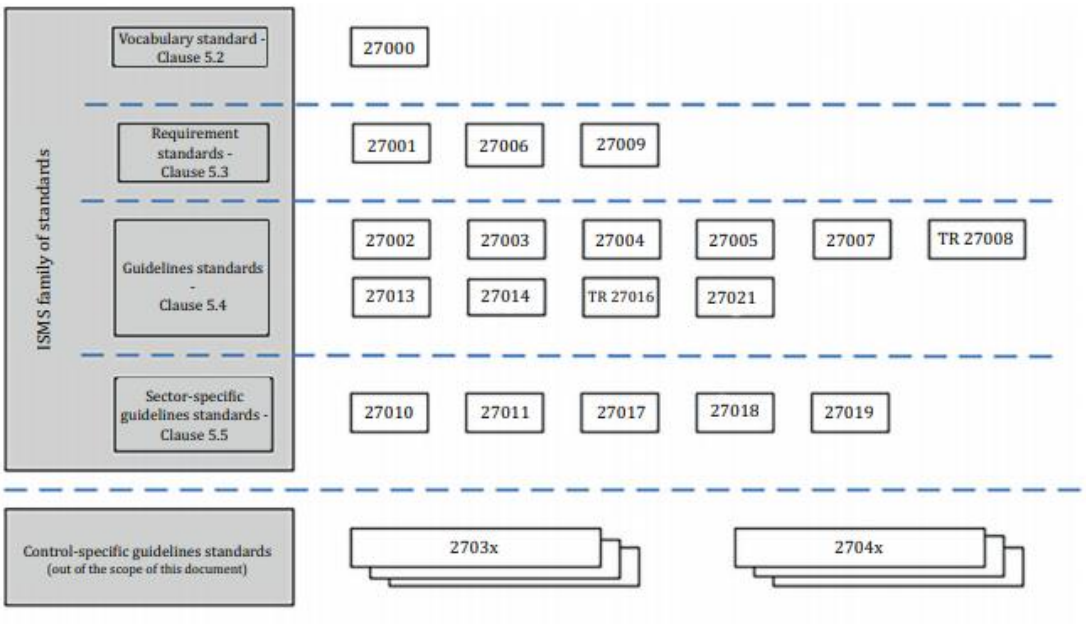

Figura 2. Familia ISO 27000 [8].

1.1.4 Norma ISO / IEC 27001

La primera integrante de la norma ISO 27000 es un estándar publicado por la Organización Internacional para la normalización (ISO) en octubre de 2005, esta norma contiene parámetros que son empleados para elaborar un SGSI, las normas que contiene abarcan todo tipo de situación o inconveniente que pueda suscitarse en un departamento o institución partiendo de una evaluación de riesgos analizando el impacto que ocasionan, luego se plantea una táctica para mitigar los riesgos [2]. El aspecto relevante de la norma ISO 27001 es que contiene las especificaciones y procesos para elaborar el SGSI que proteja la confidencialidad e integridad del lugar donde se implemente, pero no instaura el modo de implementar los controles de seguridad.

Este documento especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI); no es una especificación técnica y no especifica ninguna medida de seguridad específica. En cambio, el estándar describe un marco que las empresas pueden seguir para analizar y minimizar el riesgo de seguridad de su información. Empresas de todos los tamaños e industrias pueden mejorar la protección de sus activos más importantes, es decir, su información cumpliendo con la norma ISO 27001. [8].

La norma ISO / IEC 27001 [12], se centra en resguardar la confidencialidad, seguridad y disponibilidad de la información en una empresa, esto se hace identificando posibles áreas problemáticas recolectando información y realizando una evaluación de riesgos y luego determinar los pasos necesarios para implementar un sistema que permita mitigar las vulnerabilidades. La implementación de la norma ISO / IEC 27001 está relacionada con el establecimiento de reglas organizacionales, es decir, el desarrollo de documentos procedimientos que son necesarios para prevenir violaciones en el sistema de seguridad. Dado que esta implementación requerirá gestionar múltiples políticas, procedimientos, personas y activos.

1.1.5 Norma ISO / IEC 27002

La norma ISO/IEC 27002:2013 proporciona requisitos de mejores prácticas es la segunda norma internacional más importante cuando se trata de introducir un SGSI en una empresa. En combinación con ISO/IEC 27005:2018, que describe la prevención de riesgos (RMP) para la seguridad de la información, se tratan los criterios evaluar, priorizar y aceptar riesgos. La aplicación del RMP la emplean en los gestores de riesgos, quienes asumen la responsabilidad de los riesgos residuales de los "activos de respaldo". Si los riesgos no se gestionan correctamente desde el principio, un proyecto puede encontrar problemas incluso antes de comenzar [13]. La ISO/IEC 27002 tiene un control específico para la gestión de activos que será útil en esta investigación con el fin de elaborar el inventario.

La norma ISO 27002 está estrechamente vinculada a la norma ISO 27001. Contiene reglas de referencia para la seguridad de la información, la ciberseguridad, la protección de datos y el apoyo a la implementación. Se basa en las mejores prácticas reconocidas mundialmente. La norma ISO 27001 especifica los objetivos que debe cumplir una empresa para conseguir la certificación. La ISO 27002 para lograr estos objetivos describe las medidas del Anexo A de la ISO 27001 que deben implementarse en la empresa.

En un principio el control 8.1.1. indica que se deben identificar los activos asociados con la información y se debe elaborar y mantener un inventario de activos. Siguiendo con lo que dice la norma el control 8.1.2. señala que los activos deben tener un propietario. El control 8.2.1. indica que la información se debe clasificar en función de los requisitos

legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada. Los controles pertenecientes al numeral A8 serán útiles para cumplir con los objetivos de esta investigación [14].

1.1.6 Declaración de Aplicabilidad (SoA)

Una Declaración de Aplicabilidad, también conocida como SoA, es un documento que evalúa los riesgos de seguridad de una organización e identifica los controles específicos implementados para mitigar esos riesgos. Por lo general, se requiere un SoA como parte de una auditoría de cumplimiento según ISO 27001 [14].

Las organizaciones utilizan declaraciones de aplicabilidad con el objetivo de demostrar su compromiso con la seguridad y demostrar que han tomado medidas para abordar sus riesgos de seguridad específicos. Por ejemplo, un posible cliente o socio comercial puede solicitar una declaración de aplicabilidad como parte de la diligencia debida. En cualquier caso, un SoA es un documento importante que puede ayudar a brindar confianza en la postura de seguridad de una organización [14].

La Declaración de Aplicabilidad contiene la totalidad del Anexo A, consta de 114 medidas divididas en 14 cláusulas de A.05 a A.18 [14]:

- A.5 Política de seguridad de la información, trata de las orientaciones generales de su política de seguridad de la información.
- A.6 Organización de la seguridad de la información. Trata de la organización interna y las normas de uso de los dispositivos móviles tanto en el trabajo como en casa.
- A.7 Seguridad de los recursos humanos. Hace referencia a la seguridad de la información en los procesos de contratación y salida, así como a las medidas que deben adoptarse durante la vigencia del contrato.
- A.8 Gestión de activos. Se abordan las responsabilidades y normas de gestión de los activos (todos los bienes e información de la empresa) y la forma de clasificarlos.
- A.9 El control de acceso. Propone medidas organizativas y técnicas para proporcionar un acceso seguro y adecuado a la información.

- A.10 Criptografía. Trata de las medidas criptográficas que deben establecerse para proteger sus comunicaciones y datos sensibles. También trata de las claves de cifrado.
- A.11 Seguridad física y medioambiental. Establece medidas para proteger los activos físicos, el lugar de la intrusión física y las catástrofes naturales.
- A.12 La seguridad operativa. Describe las medidas para proteger sus procesos de producción (entregar su producto o actividad, manejar cambios asociada) de los problemas de copia de seguridad, o los programas maliciosos.
- A.13 la partición de la red. Aborda la seguridad de las redes y las transferencias de información.
- A.14 Adquisición, desarrollo y mantenimiento de sistemas de información contiene medidas relativas a la protección de los sistemas de información.
- A.15 Relación con los proveedores. Trata de las medidas de protección de la información intercambiada o transmitida con los proveedores en el ejercicio de la actividad.
- A.16 La gestión de incidentes de seguridad de la información. Se refiere a la implementación de un proceso de gestión de incidentes para identificar, procesar y analizar incidentes y asegurar su trazabilidad.
- A.17 Los aspectos de seguridad de la información en la gestión de la continuidad de las actividades. Se refieren a la necesidad de seguridad en la continuidad de las actividades.
- A.18 El cumplimiento. Aborda la necesidad de asegurar que su SGSI cumple con todos los requisitos contractuales, reglamentarios y competitivos a los que la organización pueda estar sujeta.

1.2. Antecedentes de la investigación

Como resultado de una investigación relacionada con el objeto de estudio (“Sistema de gestión de seguridad de la información basado en la norma ISO 27001”). La metodología empleada para esta investigación se basó en una búsqueda científica utilizando la cadena de investigación: (‘ISO 27001’) OR (‘ISO 27002’) AND (‘asset inventory’) AND (‘security of the information’) AND (‘ISMS’). La cadena de búsqueda fue aplicada en bases de datos como ACM, Web of Science, IEEE Xplore y Elsevier. Los 6 estudios recuperados corresponden a un periodo de tiempo de entre 2018 y 2021.

El primer estudio [15], en el año 2020 presentó “Prototipo de Seguridad para Determinar Información Crítica y Mejorar la Gestión de una Organización Pública” con el objetivo de presentar un prototipo de seguridad con el propósito de identificar información crítica y optimizar la gestión de una institución pública, se utilizó el método deductivo y la investigación exploratoria, como resultado de la investigación se presentó un prototipo hibrido para controlar la información crítica, una arquitectura de seguridad mixta que permite identificar las vulnerabilidades y los riegos para mantener un control de estos. Se concluyó, que el prototipo le permite a la empresa pública controlar la seguridad de la información mitigando los riesgos y la arquitectura híbrida permite correlacionar los riesgos y verificar la identidad de los datos.

Este estudio resalta las características y ventajas de la metodología Magerit y Octave, en los resultados y conclusiones se refleja lo efectivo de ambos métodos para controlar la seguridad de la información, fue útil con el fin de escoger la metodología con el fin de evaluar el impacto de los activos de información de la PUCE-E.

El segundo estudio [5], en el año 2018 presentó “Beneficios de implementar un SGSI según a la Norma ISO 27001 en el Ecuador industria manufacturera” con el objetivo de implementar un sistema gestión de la seguridad (SGSI) según la norma ISO 27001, aplicando las metodologías de Deming (PDCA) que consta de cuatro etapas con el propósito de reevaluar procesos constantemente de tal forma que se obtenga un progreso continuo y la metodología Magerit II para analizar y administrar los riesgos. Los resultados de la investigación se explican en un estudio de caso donde se determinaron los activos relevantes de la institución, se elaboraron tablas para evaluar el impacto, determinar las amenazas, evaluar los riegos y planear como tratarlos; se obtuvieron beneficios como una mejora en la que se almacena la información, se mitigaron los riesgos a niveles aceptables, se determinaron roles y responsabilidades para mejorar la seguridad de la información. En conclusión, la norma ISO 27001:2013 es uno de los mejores modelos debido a las pautas de seguridad que garantizan la seguridad de la información, es importante obtener un diagnóstico efectivo en los procesos críticos de la organización para implementar un SGSI utilizando los recursos necesarios; el constante monitoreo de los controles, métricas y procesos es fundamental para la mejora continua del sistema.

Este estudio es interesante porque se centra en los procesos críticos de una empresa, además muestra el proceso paso a paso para diseñar el SGSI, pero lo más importante es que recalca la importancia de la mejora continua del sistema y utiliza la metodología PDCA, sería interesante aplicar esta metodología para garantizar que el análisis que se presentará a la PUCE-E se actualice constantemente con el fin de obtener la mejor versión.

El tercer estudio [16], en el año 2018 realizó una "Propuesta de metodología de gestión de riesgos de TIC para entidades gubernamentales basada en ISO / IEC 27005", tiene como objetivo de plantear una metodología para mitigar los ataques y delitos cibernéticos que se dan en varias instituciones públicas del Ecuador, estas entidades han experimentado varias vulnerabilidades en los sistemas informáticos que utilizan y en las páginas web debido a que no cumplen con normas de seguridad, se determinó que las entidades gubernamentales deben implementar un SGSI aunque puede llevar muchísimo tiempo. La metodología usada para proponer esta herramienta está basada en los lineamientos de la ISO 27005 como resultado se obtuvo una metodología de cuatro etapas que contienen varias actividades, que permiten establecer un contexto, identificar, estimar y evaluar los riesgos; este proceso fue aplicado en el caso de una entidad pública de Ecuador. Se concluyó que la metodología empleada facilita identificar activos, riesgos y aplicar controles del SGSI para la entidad pública, pero es recomendable que un experto sea parte del grupo que implementará la metodología, especialmente al tratar los riesgos.

La metodología propuesta en este estudio sin duda tiene varias ventajas, pero principalmente en el factor tiempo, puesto que al ser una guía que funciona por etapas y cada una de estas contiene actividades que representan una función importante dentro del proceso, el tiempo en el que se diseñe un SGSI con esta metodología será más corto teniendo todos estos pasos a seguir.

El cuarto estudio [12], en el año 2020 se realizó "Problemas de implementación de sistemas de gestión de seguridad de la información" el objetivo de este estudio es explicar los problemas que se pueden dar en el proceso de implementar un SGSI y dar sugerencias con el objetivo de evitar o solucionar los incidentes. La metodología de este documento consiste en listar los pasos para implementar el SGSI con la norma ISO 27001:2013. Como resultado de esta investigación se tienen varios sucesos que pueden darse al implementar el SGSI como inconformidades por parte de la alta dirección, el tiempo que

toma implementar el sistema y limitaciones del enfoque propuesto por la norma ISO 27001 como tener pocos detalles en los requisitos. En conclusión, los problemas que justifican los gastos en seguridad de la información y la eficacia de sus actividades son cada vez más relevantes, es necesario evitar la duplicación de los procesos de seguridad de la información, elevar la protección de la información a un nivel cualitativamente nuevo; implementar el estándar de seguridad ISO 27001 soluciona todos los inconvenientes que se puedan ocurrir al implementar un sistema para proteger la confidencialidad de una empresa.

Esta investigación es importante porque no siempre se obtienen los resultados esperados y es bueno conocer los problemas que pueden ocurrir al implementar un sistema gestión de seguridad de la información para identificar las fallas en el proceso de diseño o implementación para tenerlas en cuenta al elaborar al analizar el sistema de gestión de seguridad de información para la PUCE-E y no cometer los mismos errores.

El quinto estudio [7], en el año 2020 se presentó "Evaluación de la madurez de la seguridad de la información organizacional basada en ISO 27001 e ISO 27002" el objetivo de este estudio es desarrollar una metodología práctica para realizar la evaluación de la madurez de la seguridad de la información para las instituciones. La metodología utiliza un método comparable a COBIT 5 para evaluar el nivel de madurez de los controles de seguridad y las cláusulas de la norma ISO 27001: 2013 y aprovecha las directrices de la norma ISO 27002: 2013. El resultado de la evaluación son reglas y recomendaciones para mejorar el SGSI, que se pueden utilizar para la toma de decisiones y planes estratégicos, así como insumos para la gestión de riesgos de seguridad de la información de la organización. En conclusión, la evaluación se puede realizar periódicamente para capturar los cambios organizacionales que impactan los objetivos del SGSI y para tomar decisiones estratégicas y tácticas sobre el desempeño de las operaciones de seguridad.

La investigación analiza que puede mejorar en un SGSI, al hacer la parte práctica seguramente ya habrá reglamentos para proteger la seguridad de la información, conocer el proceso de evaluación de la madurez de un SGSI podría ser útil para ver que tan bien aplicadas están las métricas implementadas.

El sexto estudio [9], en el año 2018 se realizó "Sobre el desarrollo del marco del sistema de gestión de seguridad de la información (SGSI) para el centro de datos basado en ISO

27001", el objetivo de este estudio es implementar un SGSI con el propósito de identificar y reducir los riesgos en un centro de datos de tal forma que la protección sea física y lógica, se requiere que se evalúen los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad. La metodología utilizada emplea información relacionada con el SGSI, también se observó seis centros de datos y se realizaron entrevistas con el fin de obtener recomendaciones de los parámetros de seguridad que deben ser implementados. Se obtuvo el marco de SGSI deseado que se comparó con el marco SGSI de una empresa de telecomunicaciones, como resultado, se demostró que el SGSI propuesto posee más beneficios que el otro. En conclusión, se desarrolló un marco SGSI específico para un centro de datos con el Anexo A de la norma ISO 27001, que integra 21 controles para preservar la seguridad de la información.

La investigación se centra en la seguridad de la información con el objetivo de analizar un SGSI usando la norma ISO 27001. El tema es similar al tema de investigación de este documento, permite tener una noción de aspectos importantes como conocer dónde se implementará el SGSI y la importancia de entrevistar a las personas que trabajan día a día en este lugar para conocer que recomendarían con el fin de mitigar los riesgos y aplicar los controles.

CAPÍTULO II: METODOLOGÍA

2.1. Delimitación de la investigación

Esta investigación se desarrolló con el objetivo de analizar un sistema de gestión de seguridad de la información para la Pontificia Universidad Católica del Ecuador Sede Esmeraldas. La delimitación espacial del proyecto se destina a varios departamentos de la universidad de Esmeraldas, calle Espejo y subida a Santa Cruz. En cuanto a la delimitación temporal sé consideraron los datos documentados dentro del periodo de 2022-2024, basado en el proceso que realizan con el objetivo de mantener la integridad y seguridad de la información utilizando la norma ISO 27001. La delimitación del universo serán las personas seleccionadas de cada departamento, a quienes se entrevistó.

2.2. Tipos de investigación

El primer tipo de investigación utilizada es la investigación bibliografía para elaborar un marco teórico esencial que define los conceptos necesarios referentes a seguridad de la información, el estándar ISO 27001, se emplearon artículos obtenidos de bases de datos científicas de proyectos similares.

Este estudio se realizó empleando una investigación descriptiva para especificar las características de la población, cualitativa para recopilar y analizar los datos obtenidos en las entrevistas y cuantitativa para analizar los datos numéricos; se evaluaron y detallaron los procesos críticos de la Pontificia Universidad Católica del Ecuador Sede Esmeraldas, describiendo las medidas empleadas mediante la norma ISO/IEC 27002. Se realizaron varias entrevistas al personal de la universidad con el fin de evaluar el impacto de materializarse las amenazas en los activos de información.

2.3. Métodos y técnicas

2.3.1 Métodos

En esta investigación se usaron varios métodos para recolectar los aspectos relevantes sobre los activos de la PUCE-E.

El método descriptivo se utilizó para realizar la investigación porque implica observar y describir el proceder de un individuo o situación, se explica de forma general

el proceso con la finalidad de levantar información, se analizaron los datos obtenidos con la metodología utilizada para elaborar el inventario de activos y se elaboró una declaración de aplicabilidad.

El método inductivo también se utilizó, se establecieron conclusiones generales en base a los datos obtenidos al aplicar las técnicas que se aplicarán al personal de los departamentos.

2.3.2 Técnicas

La técnica empleada para obtener la información necesaria de los departamentos que administran la información crítica de la PUCE-E, constaron de entrevistas al personal administrativo, cada una se desarrolló acorde a las áreas, se realizó un formulario de preguntas con el fin de completar el inventario, con esta técnica se determinaron los procesos que usan en los departamentos al gestionar la información y se recolectaron las características de los activos.

La técnica de observación fue fundamental en esta investigación para observar los procesos, activos, el impacto con el fin de analizar y comparar los datos.

2.4. Población y muestra

La población de esta investigación fue una persona de cada departamento de la PUCE-E como se detalla en la Tabla 1, las cuales dieron su punto de vista sobre los procesos y los activos del departamento según la función que desempeñen dentro de este. Para la investigación no se incluyeron todos los departamentos de la universidad, se seleccionaron solo los que gestionan información referente a la data.

Tabla 1. Personal administrativo

Departamento de TI	
Departamento	**Cargo**
Departamento de TI	Jefe de departamento
Secretaria General	Secretario General
Dirección Académica	Asistente Académica
Dirección de estudiantes	Directora de Estudiantes
Unidad de Educación Continua	Coordinadora de Educación Continua
Departamento Medico	Médico Ocupacional

Departamento de Comunicaciones	Responsable
Biblioteca	Responsable

2.5. Descripción de instrumentos

Para la recolección de datos del presente proyecto de investigación, acerca de las variables a tomar en cuenta con las cuales se desarrolló la investigación y ejecución, se utilizaron dos instrumentos, los cuales fueron: entrevista y una tabla.

Como primer instrumento se utilizó la entrevista a una persona de cada departamento seleccionado de la PUCE-E, se elaboró un cuestionario de quince preguntas que puede observarse en el Anexo 1, las dos primeras con el fin de identificar procesos y activos, de la tercera a la octava pregunta se obtuvieron las características de cada activo de información. De la novena a la décimo quinta pregunta se hicieron preguntas con el fin de evaluar los tres pilares de la seguridad de la información confidencialidad, integridad y disponibilidad.

La Tabla 4 está enfocada en obtener los datos para el inventario de activos, ha sido diseñada con los parámetros que indica la metodología propuesta por la ISO/IEC 27002, del dominio 8 se utilizaron los objetivos de control 8.1 y 8.2; también sé utilizo de la ISO/EC 27005 del Anexo B el control B.1 y B.3. En la Tabla 2 se justifica las razones de obtener la información de los controles específicos que se han utilizado.

Tabla 2 Controles de la norma ISO 27002 e ISO 27005.

Campo	Respuesta	Justificación
Código TI	Código para identificar los activos	**"ISO 27002. 8.2.2 Etiquetado de la información.** Los activos deben estar claramente identificados y debería elaborarse y mantenerse un inventario. Debería desarrollarse e implantarse un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización. Las etiquetas deberían ser fácilmente reconocibles" [14].
Activo	Nombre del activo	**"ISO 27002. 8.1.1 Inventario de activo**s. La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deberían estar claramente identificados y debería elaborarse y mantenerse un inventario" [14].

Propietario	Propietario del activo	**"ISO 27002. 8.1.2 Propiedad de los activos.** Todos los activos que figuran en el inventario deberían tener un propietario" [14].
Descripción del activo	Breve descripción de lo que contiene el activo	**"ISO 27005. B.1.3 Lista y descripción de los activos de respaldo**. El alcance consta de activos que deben identificarse y describirse" [17].
Tipo de activo	Tipos de activos	**"ISO 27005. B.1. Ejemplos de identificación de activos.** Para realizar una valoración de activos, una organización primero necesita identificar sus activos" [17].
Área/proceso	Departamento o proceso al que pertenece el activo	**"ISO 27002. 8.1.1 Inventario de activos.** La organización debería identificar los activos relevantes para el ciclo de vida de la información y documentar su importancia. El ciclo de vida de la información debería incluir la creación, tratamiento, almacenamiento, transmisión, borrado y destrucción" [14].
Ubicación de activo	Lugar donde se encuentra el activo	**"ISO 27002. 8.1.1 Inventario de activos.** La organización debería identificar los activos relevantes para el ciclo de vida de la información y documentar su importancia. El ciclo de vida de la información debería incluir la creación, tratamiento, almacenamiento, transmisión, borrado y destrucción" [14].
Medio de conservación físico y/o digital	Verificar como se almacena el activo	**"ISO 27002. 8.2.1 Clasificación de la información**. La información debería ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, otros activos pueden ser clasificados considerando la clasificación de la información que almacenan, procesan o cualquier otra forma de protección o tratamiento por el activo" [14].
¿Hay datos sensibles?	Obtener información para saber si hay datos sensibles	**"ISO 27002. 8.2.1 Clasificación de la información.** La información debería ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas" [14].
¿Hay datos personales?	Obtener información para saber si hay datos personales	**"ISO 27002. 8.2.1 Clasificación de la información**. La información debería ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, otros activos pueden ser clasificados considerando la clasificación de la información que almacenan, procesan o cualquier otra forma de protección o tratamiento por el activo" [14].

Responsable	Quien es el responsable del activo	**"ISO 27002. 8.1.3 Uso aceptable de los activos.** Debería concienciarse a los usuarios, tanto empleados como externos que usen o tengan acceso a los activos de la organización. Deberían ser responsables del uso que hagan de los recursos de tratamiento de información y cualquier otro uso hecho bajo su responsabilidad" [14].
Usuarios	Que usuarios utilizan cada activo	**"ISO 27002. 8.1.3 Uso aceptable de los activos.** Debería concienciarse a los usuarios, tanto empleados como externos que usen o tengan acceso a los activos de la organización" [14].
Correlación	Relación entre activos (Activos que se generan de otro activo)	Esta sección fue adaptada acorde a las necesidades de la institución.
Clasificación por confidencialidad	Clasificación	**"ISO 27002. 8.2.1 Clasificación de la información**. La información debería ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, otros activos pueden ser clasificados considerando la clasificación de la información que almacenan, procesan o cualquier otra forma de protección o tratamiento por el activo" [14].
Nivel de impacto	Evaluación del impacto mediante la confidencialidad, integridad y disponibilidad.	**"ISO 27002. 8.2.1 Clasificación de la información.** Los resultados de la clasificación deberían indicar el valor de los activos en función de su sensibilidad y criticidad para la organización, por ejemplo, en términos de su confidencialidad, integridad y disponibilidad [14]. **ISO 27005. B.3 Evaluación de impacto.** Se considera que el impacto tiene un efecto inmediato (operacional) o un efecto futuro (comercial) que incluye consecuencias financieras y de mercado" [17].

Los datos del inventario se registraron en una tabla compuesta por un código que identifica a cada activo, este código se compone por una letra A (Activo) y tres números empezando por el "001"; la numeración va aumentando de forma ascendente a medida que se va agregando cada activo. Luego sigue la sección del nombre del activo, donde se indica el nombre de cada uno, después la columna para indicar quién es el propietario, que puede ser el departamento donde se encuentra o el cargo de quien es responsable del activo.

Después se describe que información almacena o contiene el activo, se indica el tipo de activo de información que puede ser una aplicación web, una base de datos, un proceso,

un informe, un servidor, un firewall, un documento o imágenes. Parte importante de esta tabla es la sección de área o proceso, se detalla el proceso en el que se emplea el activo o el área en el que se usa, luego está la ubicación del activo donde se indica si el activo está en la nube, en un servidor, en una página web o departamento de la institución. Después, se presentan campos que permitieron levantar información sobre el medio donde se conservan los activos de información, ya sea físico y/o digital; luego la sección para conocer si el activo contiene datos sensibles, datos personales o ambos.

El siguiente campo se usó para indicar al responsable funcional y al informático, en la mayoría de los activos hay un responsable que se encarga de utilizar el activo, pero también de mantenimiento informático. La siguiente sección tiene el fin de conocer los usuarios que pueden acceder a la información del activo, como estudiantes, profesores, personal administrativo, estudiantes prospectos, exestudiantes y la ciudadanía en general. La columna data describe la correlación entre los activos, también hay una sección con el objetivo de clasificar la información por confidencialidad que puede ser pública reservada, pública clasificada. Por último, se evaluaron los activos mediante los tres parámetros de seguridad de la información: confidencialidad, integridad y disponibilidad; cada uno de estos pilares se calificaron en una escala del 1 (muy bajo) al 5 (muy alto) y luego se sumó cada valor para obtener el nivel de impacto.

2.6. Técnicas de procesamiento y análisis de datos

En el análisis de los datos se empleó la estadística descriptiva, que es una técnica para recolectar, almacenar y organizar los datos obtenidos mediante los instrumentos.

Las entrevistas se detallan a partir del análisis narrativo con el objetivo de detallar los procesos y activos que utilizan al gestionar la información en los departamentos seleccionados. Se utilizó una tabla diseñada para tabular los datos obtenidos, identificar los datos con un código único, detallar sus características y evaluar el impacto aplicando la metodología de la ISO/IEC 27002. Por último, se presentaron los datos a través de gráficos estadísticos para hacer una comparación visual de los resultados, para esto se agruparon los activos por el tipo de activo.

2.7. Normas éticas

Esta investigación titulada “análisis de un sistema de gestión de seguridad de la información para la PUCE-E basado en la norma ISO 27001”, fue desarrollada bajo las normativas establecidas por la Pontificia Universidad Católica del Ecuador Sede Esmeraldas. También se respetaron los derechos de autor correspondientes a los trabajos relacionados con esta investigación tomadas de bases de datos científicas.

Por la sensibilidad y confidencialidad de los datos, se trataron con total discreción, integridad y profesionalismos; esta información no se utilizará para otros fines que no sean educativos.

CAPÍTULO III: RESULTADOS

El propósito de esta investigación fue conocer los activos de información de la PUCE-E con el objetivo de evaluar el nivel de impacto, en esta sección se muestran los resultados obtenidos al realizar varias entrevistas al personal administrativo de la universidad; primero se identificaron los activos y se hizo un análisis acorde a sus características, después se evaluó el nivel de impacto el cual es representado mediante una tabla y varios gráficos para analizar por los tipos de activos más utilizados, por ultimo está el análisis de la declaración de aplicabilidad.

3.1 Identificación de los activos de información

Primero se obtuvo un permiso del Jefe del departamento de Talento Humano luego se reservó las citas con una persona de cada departamento, esto tomó una semana. Las entrevistas se realizaron al Jefe del Departamento de TI, al Secretario General, a la Directora de Estudiantes, a la Asistente Académica, a la Coordinadora de la unidad de educación continua, al Médico Ocupacional y a la Responsable de Biblioteca. El proceso de entrevistas tomo aproximadamente tres semanas siguiendo un cronograma acorde a la disponibilidad de los entrevistados.

En las entrevistas se pudo conocer los activos de información que utilizan en cada departamento, también se especificó varias características de cada activo como el propietario y los responsables de cada activo. Se mencionó que un activo puede tener responsables funcionales o informáticos, por lo general todas las personas del departamento pueden usarlo, pero en cuanto a funciones operativas o de soporte, el responsable es el departamento de TI de la PUCE-E.

La mayoría de los activos son aplicaciones web, bases de datos, reportes y documentos; en su mayoría se conservan en digital, se encuentran en la nube, en un servidor o en OneDrive y algunos se almacenan en físico, en carpetas dentro del departamento correspondiente.

Los usuarios que usan los activos de información de la PUCE-E son el personal administrativo; el acceso a estudiantes y docente es limitado, a las aplicaciones web necesarias para el registro de notas, pagos, control de tareas y comunicación de noticias; los usuarios prospectos, exestudiantes y ciudadanía tienen un acceso limitado.

3.2 Evaluación del nivel de impacto de los activos

A continuación, la Figura 3 con un listado de los tipos de activos de información con su respectiva cantidad, suma 66. La tabla con el inventario de activos y la evaluación del nivel de impacto completa está en el Anexo 3.

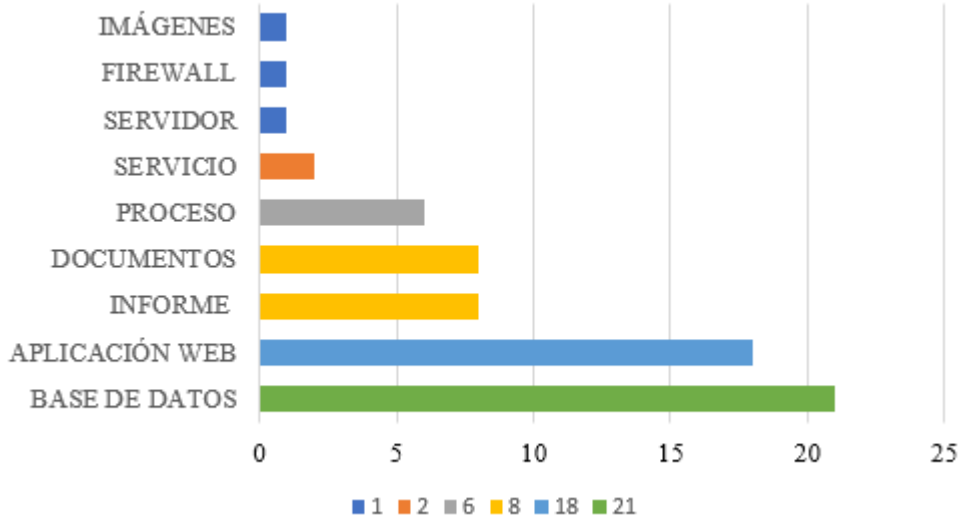

Figura 3. Tipos de activos.

Se recopiló la información de 66 activos, al analizar los tipos se comprobó que la mayoría de los activos de información son de tipo base de datos, también hay varios de tipo aplicación web.

En el Anexo 3. Tabla de evaluación del nivel de impacto de los activosestá la Tabla 6 con todos los activos indicando el valor de confidencialidad, integridad, disponibilidad y el nivel de impacto del riesgo para la seguridad de la información que tendrían en la universidad. La tabla refleja que en la mayoría de los activos hay un nivel de impacto de medio a alto, sus valores están entre 2 y 5, demostrando cuales activos son los activos a los que se debería implementar medidas de seguridad.

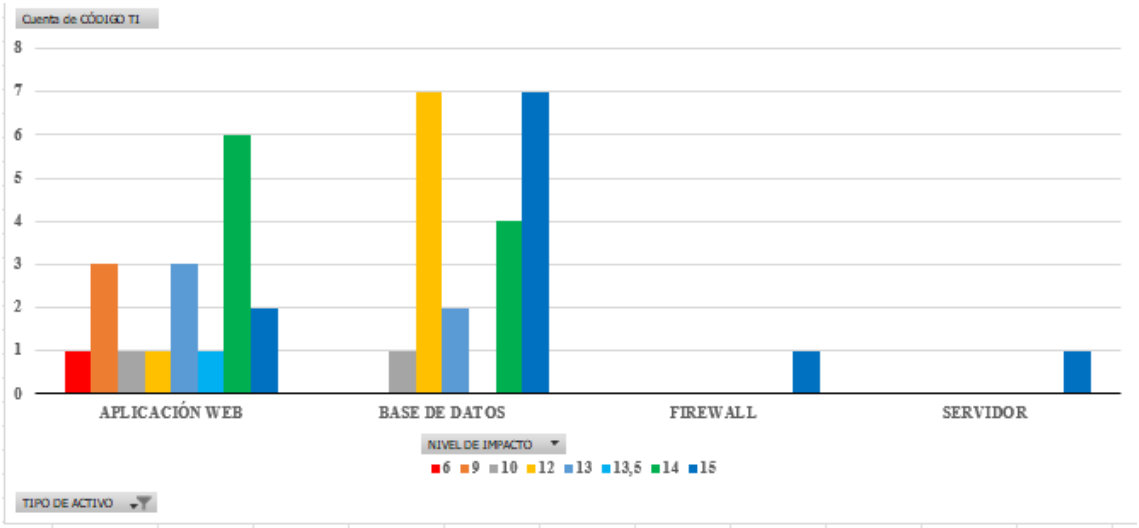

Figura 4. Análisis de tipos de activos.

En la Figura 4 se observa que 6 de aplicaciones web tienen un nivel de impacto 14, 3 tienen un nivel de impacto 9 y 3 un nivel de impacto de 14; la mayoría poseen un nivel de impacto alto, demostrando la necesidad de implementar controles que permitan salvaguardar la seguridad de las aplicaciones. Hay 21 activos que son de tipo base de datos se puede observar que 1 activo tiene un nivel de impacto 10, 7 activos tienen un nivel de impacto 12, 2 activos tienen un nivel de impacto 13, 4 activos tienen un nivel de impacto 14 y 7 activos tienen un nivel de impacto 15. La mayoría de los activos tipo base de datos tienen un nivel de impacto 12 y 15, es un nivel alto. El tipo de activo Firewall y Servidor tienen ambos un activo con un nivel de impacto de 15, el nivel más alto.

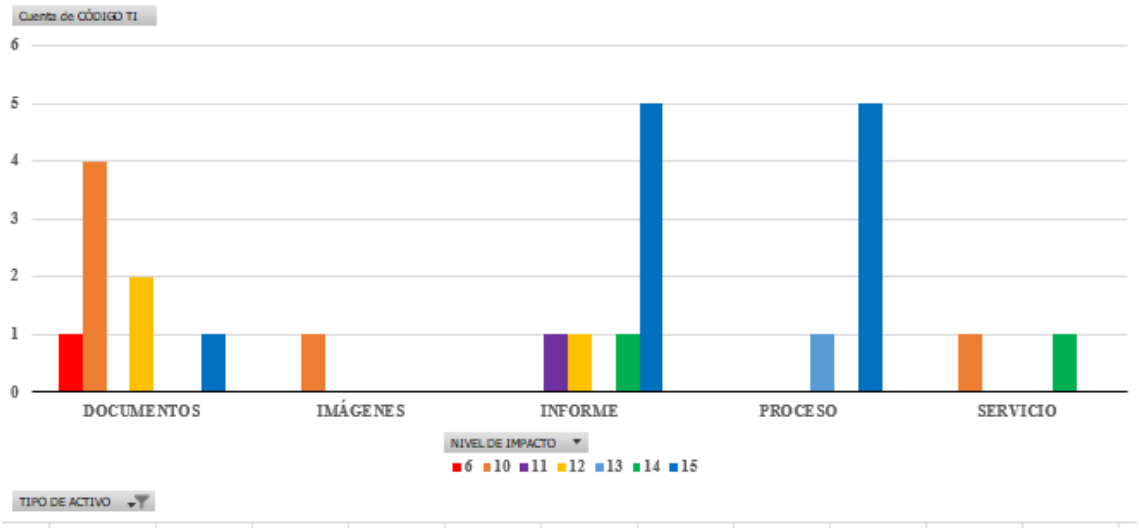

Figura 5. Análisis de tipos de activos.

En la Figura 5 se aprecia que en los documentos solo 1 activo tiene nivel de impacto 15 y 4 de los activos tienen un nivel de impacto 10. Las imágenes tienen un nivel de impacto de 10. En los informes 5 activos tienen un nivel de impacto de 15, la mayoría tienen un nivel de impacto alto. Los procesos tienen 5 activos con nivel de impacto de 15, es alto. Los servicios tienen un nivel de impacto de 10 o de 14, es alto.

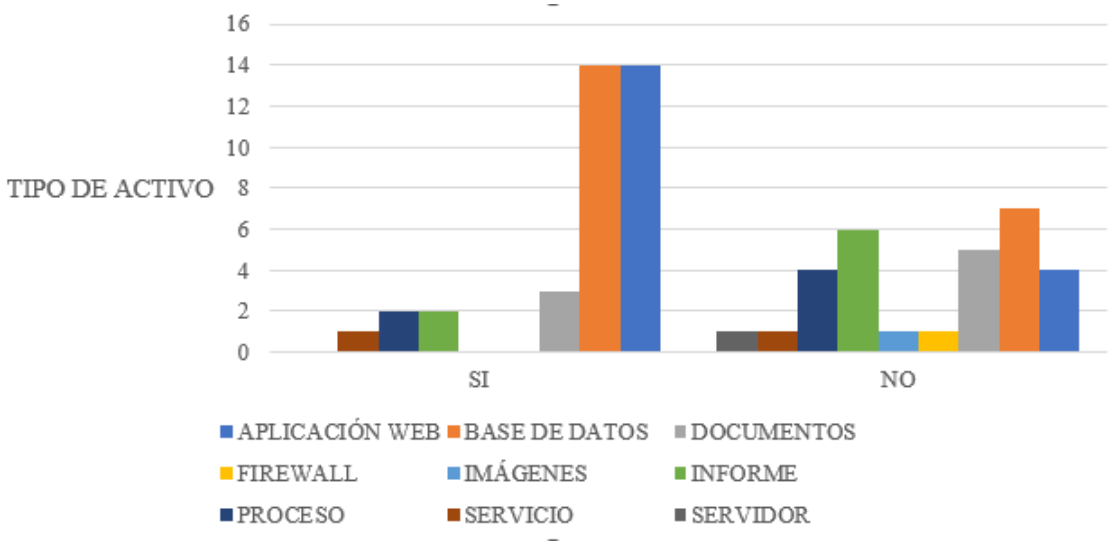

Figura 6. Datos sensibles.

En la Figura 6 se observa que las aplicaciones web y las bases de datos tienen más datos sensibles y los servicios tienen menos.

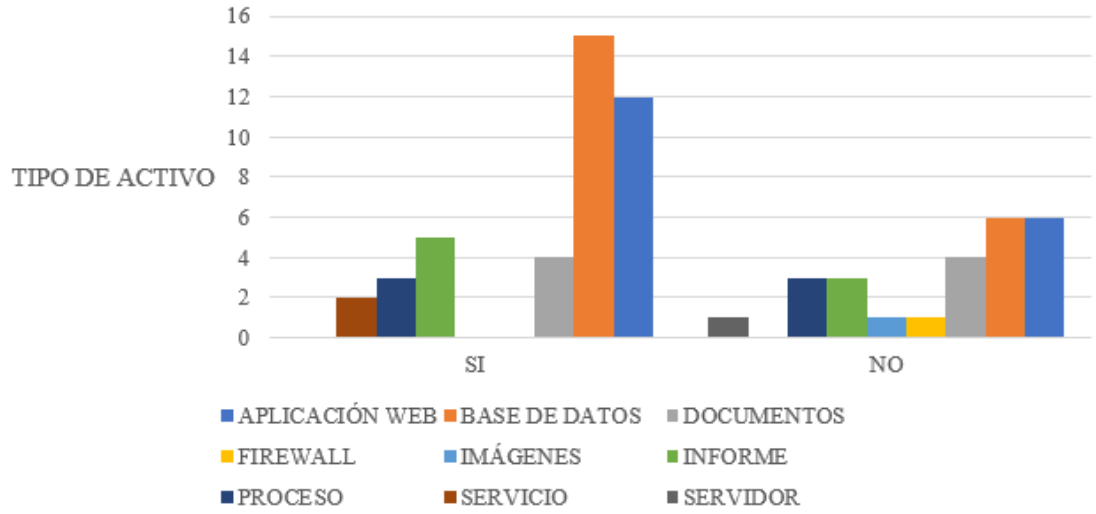

Figura 7. Datos personales.

Se observa en la Figura 7 que las bases de datos son el tipo de activo con más datos personales reuniendo 15, siguen las aplicaciones web con 12, en los informes también se puede encontrar información clasificada como personal.

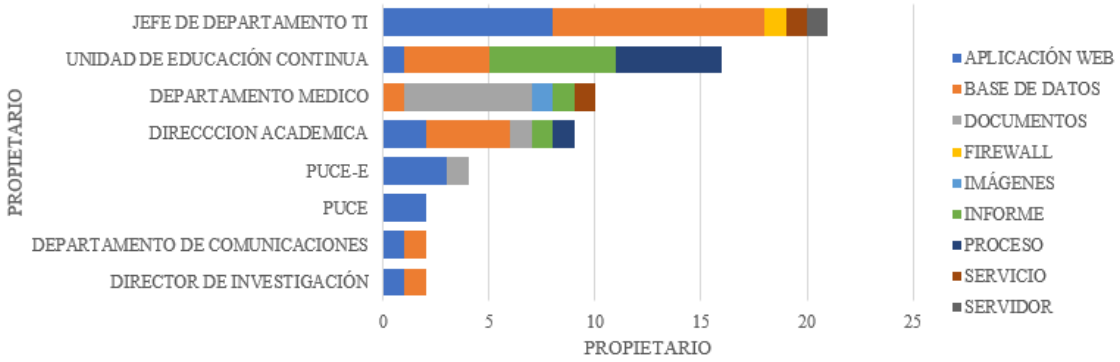

Figura 8. Análisis de los propietarios.

En la Figura 8 se aprecia que el jefe del departamento de TI es el propietario de la mayoría de los activos y el departamento de Unidad de Educación Continua también tiene muchos activos analizados en esta investigación.

3.3 Declaración de aplicabilidad.

El objetivo de esta sección es indicar un análisis de la Tabla 3 de cuáles son los controles de la ISO 27001 que se pueden aplicar en la institución. El documento completo está en el Anexo 4.

Tabla 3. Controles aplicables de la norma ISO 27001 a la PUCE-E basado en [14].

Control	Se implementa (%)	No se implementa (%)
A.5. Políticas de seguridad de la información	0	100
A.6. Organización de la seguridad de la información	0	100
A.7. Seguridad relativa a los recursos humanos	66,7	33,3
A.8. Gestión de activos	0	100
A.9. Control de acceso	61,5	38,5
A.10. Criptografía	0	100
A.11. Seguridad física y del entorno	53,3	46,7
A.12. Seguridad de las operaciones	42,9	57,1
A.13. Seguridad de las comunicaciones	42,9	57,1
A.14. Adquisición, desarrollo y mantenimiento de los sistemas de información	46,2	53,8

A.15. Relación con proveedores	40	60
A.16. Gestión de incidentes de seguridad de la información	28,6	71,4
A.17. Aspectos de seguridad de la información para la gestión de la continuidad del negocio	0	100
A.18. Cumplimiento	12,5	87,5
Total de cumplimiento / no cumplimiento	**35,4**	**64,6**

Analizando la declaración de aplicabilidad se obtiene un porcentaje de 35.4% de normas que se aplican de forma informal en la institución a pesar de no contar con un sistema de gestión de seguridad de la información. El 64.6% restante indica los objetivos de control que no sé han implementado.

CAPÍTULO IV: DISCUSIÓN

El análisis de la seguridad de la información de la PUCE-E obtenido con entrevistas al personal administrativo, busca identificar los activos de información y evaluar su impacto utilizando la seguridad de la información. Los activos de información de la universidad como lo demostraron los resultados en su mayoría tienen un valor de nivel de impacto muy alto, esto se debe a que la mayoría contiene información sensible o personal.

En el primer estudio [15] se analizó un prototipo de seguridad con el objetivo de determinar información crítica y mejorar la gestión de una organización pública, en los resultados de esta investigación comparan Octave y Magerit que son dos metodologías para la gestión de riesgo, demuestran que el uso de una metodología hibrida puede ser efectiva con el fin de adaptarse mejor a la institución. En esta investigación se usó la metodología de la ISO 27005 que es muy similar a la metodología de Magerit.

Según el estudio [5] afirma que la norma ISO 27001 es uno de los modelos de mejores prácticas y pautas de seguridad más apropiados con el fin de establecer una serie de estrategias y controles que aseguren la información y sus beneficios. El método usado para elaborar el inventario de activos y la tasación fue el mismo que utilizaron en esta investigación, en el que se toma como parámetros la confidencialidad, integridad y disponibilidad con el fin de evaluar el nivel de impacto de los activos. Ambas investigaciones tuvieron un nivel de impacto de los activos de alto nivel y deben tener medidas de protección para no ser vulnerados. Los activos con los que cuenta cada institución son diferentes acordes a sus recursos, pero ambas tienen en común el tipo de activo servidor y aunque en [5] se analizan específicamente ciertos sistemas, en esta investigación se analizaron, pero se clasifican en la categoría de aplicaciones web. En este análisis se obtuvo un nivel de impacto de 15 para la categoría servidor mientras que en [5] el servidor tuvo un nivel de impacto de 14, ambos tienen un nivel de impacto muy alto que puede generar daños de imagen o repercusiones económicas.

En la investigación [16] plantean una tabla para calificar la confidencialidad, integridad y disponibilidad, la tabla contiene un rango de valores del 1 al 5 donde 1 es muy bajo y 5 es muy alto. Esta investigación se relacionó con el tema de estudio ya que el método que utilizaron fue útil para evaluar el impacto de los activos a través de las tres dimensiones de seguridad de la información. Además, en [16] plantean una tabla con varios activos de

información que fue útil para emplear en esta investigación, pero al momento de elaborar el inventario se agregaron más tipos de activos, ya que durante las entrevistas se tomó en cuenta que en la PUCE-E tienen activos diferentes. También evaluaron un centro de datos, bases de datos, aplicaciones web, computadoras, documentos y usuarios; mientras que en esta investigación solo se evaluaron bases de datos, aplicaciones web y documentos, se tuvo que agregar más activos del tipo firewall, imágenes, informe, proceso, servicio y servidor para incluir todos los tipos de la PUCE-E

En los resultados de [12] se plantean una serie de pasos para implementar un sistema de gestión de seguridad de la información, entre estos se destaca la importancia de identificar los activos de información. Como parte de los resultados de esta investigación se elaboró un inventario de activos donde se pueden identificar con un código, están organizados por departamento y también se pueden agrupar por tipo de activo; con esto se logró identificar y clasificar los activos de información de la PUCE-E.

La clasificación de los activos por tipo de activo es utilizada en [9], utilizaron los tipos hardware, software y políticas y procedimientos, recursos humanos y organización; organizar los activos permite elaborar un análisis por cada tipo. En esta investigación se han organizado los activos acordes a su tipo, sin embargo, se utilizaron otros tipos de activos para cubrir las necesidades de la PUCE-E. En [9] los resultados muestran una forma de analizar los activos por su tipo tal y como se hizo en esta investigación, también plantearon un cuadro de sugerencias de que controles de la ISO 27001 deberían aplicarse por cada tipo de activo, esto no se hizo en esta investigación porque no era parte de los objetivos planteados.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

Conclusiones

El objetivo de identificar los activos de información de la PUCE-E se cumplió mediante entrevistas y análisis detallados, lo que permitió elaborar un inventario exhaustivo de los activos más críticos. La finalidad de evaluar el impacto de los activos se logró con la tabla del inventario de activos donde al final se hizo la evaluación, para conocer cuales son los activos que tendrán un mayor impacto sobre la economía, integridad y reputación de la universidad. El propósito de la declaración de aplicabilidad fue conocer mediante este documento cuales son los lineamientos que se cumplen y cuales faltan por aplicar en la institución.

Al evaluar los activos de información de la PUCE-E, se determinó que la mayoría de los activos de información evaluados presentan un alto nivel de impacto en caso de vulneración, esto demostró la importancia de la universidad para implementar un sistema de gestión de seguridad de la información, Los departamentos que habría que aumentar la seguridad serian el departamento de TI, secretaria general, la unidad de educación continua y dirección académica. La mayor parte de los activos contienen información personal y más de la mitad información sensible, proteger estos datos es necesario, ya que si fueran expuestos se vería afectada la integridad y prestigio de la institución.

La metodología basada en la norma ISO 27002 fue muy útil para elaborar el instrumento donde se recolectaron los datos de las entrevistas y explica detalladamente cuáles son los parámetros que debe tener un inventario de activos; además, la normativa permitió que elaborar el cuestionario de preguntas sea un proceso rápido, de hecho, tiene varias interrogantes que servían de ejemplo. Este estándar internacional define claramente las dimensiones de evaluación del impacto de los activos de información.

La importancia de la declaración de aplicabilidad suele subestimarse, pero es el documento central que define cómo implementará gran parte de la seguridad de su información; es el vínculo fundamental entre la evaluación, el tratamiento de los riesgos y la implementación de la seguridad de su información. El propósito de esta tabla es definir cuáles de los 114 controles de la norma ISO 27001 se aplicarán. El Informe de evaluación de riesgos puede ser bastante largo una organización puede identificar miles

de riesgos y dicho documento no es muy práctico en el uso diario; por otro lado, la declaración de aplicabilidad es bastante corta, tiene una línea para cada uno de los controles lo que la hace más presentable para la administración y facilita su actualización.

Una gran parte de los objetivos de control del Anexo A de la ISO 27001 no sé han aplicado en la PUCE-E, implementar un sistema de gestión de seguridad de la información formalizando los controles que si se aplican y agregando los controles que no se han implementado minimizaría los riesgos de que haya un impacto sobre los activos de información.

Recomendaciones

Considerar esta investigación que seguro será muy útil para la PUCE-E con el fin de tener un registro de los activos de información que utilizan al gestionar y almacenar la información.

Considerar la declaración de aplicabilidad que especifica que se deben aplicar controles y cuáles ya se han implementado por la institución.

La PUCE-E debería crear procesos que les permita incrementar la rentabilidad aumentando la eficiencia, incrementar la satisfacción de clientes y empleados a través de la estandarización y mejora de la calidad.

El personal administrativo que opera los activos de información debe tener conocimiento de la norma ISO 27001, para que puedan gestionar óptimamente los recurso y se minimice la posibilidad de que pueda materializarse una amenaza.

Emplear la norma ISO 27001 para implementar un sistema de gestión de seguridad de la información o aplicar una metodología que permita tener documentado el control y las políticas que deben tener para mitigar los riesgos.

REFERENCIAS BIBLIOGRÁFICAS

[1] M. Yasin, A. Akhmad Arman, I. J. M. Edward, and W. Shalannanda, "Designing information security governance recommendations and roadmap using COBIT 2019 Framework and ISO 27001:2013 (Case Study Ditreskrimsus Polda XYZ)," *Proceeding 14th Int. Conf. Telecommun. Syst. Serv. Appl. TSSA 2020*, vol. 2013, no. 95, 2020, doi: 10.1109/TSSA51342.2020.9310875.

[2] C. Hsu, T. Wang, and A. Lu, "The impact of ISO 27001 certification on firm performance," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, vol. 2016-March, pp. 4842–4848, 2016, doi: 10.1109/HICSS.2016.600.

[3] F. N. J. Solarte Solarte, E. R. Enriquez Rosero, and M. del C. Benavides Ruano, "Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001.," *Rev. Tecnológica - ESPOL*, vol. 28, no. 5, pp. 497–498, 2015, [Online]. Available: http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456/321.

[4] J. A. Lopez-Leyva, C. A. Kanter-Ramirez, and J. P. Morales-Martinez, "Customized diagnostic tool for the security maturity level of the enterprise information based on ISO/IEC 27001," *Proc. - 2020 8th Ed. Int. Conf. Softw. Eng. Res. Innov. CONISOFT 2020*, pp. 147–153, 2020, doi: 10.1109/CONISOFT50191.2020.00030.

[5] J. Velasco, R. Ullauri, L. Pilicita, B. Jacome, P. Saa, and O. Moscoso-Zea, "Benefits of implementing an ISMS according to the ISO 27001 standard in the ecuadorian manufacturing industry," *Proc. - 3rd Int. Conf. Inf. Syst. Comput. Sci. INCISCOS 2018*, vol. 2018-Decem, pp. 294–300, 2018, doi: 10.1109/INCISCOS.2018.00049.

[6] J. Aurela Pereira, "Plan de implementación de la norma ISO/IEC 27001:2005 ," Jun. 2013. Accessed: May 25, 2021. [Online]. Available: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/23704/7/jaurelaTFM0613memoria.pdf.

[7] V. Monev, “Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002,” *2020 34th Int. Conf. Inf. Technol. InfoTech 2020 - Proc.*, no. September, pp. 17–18, 2020, doi: 10.1109/InfoTech49733.2020.9211066.

[8] ISO/IEC, “INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security management systems — Overview and,” *ACM Work. Form. Methods Secur. Eng. DC, USA*, vol. 34, no. 19, pp. 45–55, 2018, [Online]. Available: http://www.worldcat.org/title/service-operation/oclc/254028066&referer=brief_results%0Ahttps://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf%0Ahttps://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf%0Ahttp://k504.kh.

[9] D. Achmadi, Y. Suryanto, and K. Ramli, “On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center,” *2018 Int. Work. Big Data Inf. Secur. IWBIS 2018*, pp. 149–157, 2018, doi: 10.1109/IWBIS.2018.8471700.

[10] H. F. Yoseviano and A. Retnowardhani, “The use of ISO/IEC 27001: 2009 to analyze the risk and security of information system assets: case study in xyz, ltd,” *Proc. 2018 Int. Conf. Inf. Manag. Technol. ICIMTech 2018*, pp. 21–26, 2018, doi: 10.1109/ICIMTech.2018.8528096.

[11] M. Arafat, “Information security management system challenges within a cloud computing environment,” *ACM Int. Conf. Proceeding Ser.*, pp. 0–5, 2018, doi: 10.1145/3231053.3231127.

[12] S. V. Aleksandrova, V. A. Vasiliev, and M. N. Aleksandrov, “Problems of implementing information security management systems,” *Proc. 2020 IEEE Int. Conf. "Quality Manag. Transp. Inf. Secur. Inf. Technol. IT QM IS 2020*, pp. 78–81, 2020, doi: 10.1109/ITQMIS51053.2020.9322896.

[13] G. S. Lampe, M. Olaru, T. E. Fogoros, and S. Massner, “Critical Success Factor for Integration of Cyber Security in Context of Managed Services,” pp. 741–748, 2022, doi: 10.24818/basiq/2022/08/098.

[14] ICONTEC INTERNACIONAL, “Norma Técnica Ntc-Iso-Iec Colombiana 27001,” no. 571, 2013, [Online]. Available: https://www.academia.edu/40913480/NORMA_TÉCNICA_NTC_ISO_IEC_COLOMBIANA_27001_TECNOLOGÍA_DE_LA_INFORMACIÓN_TÉCNICAS_DE_SEGURIDAD_SISTEMAS_DE_GESTIÓN_DE_LA_SEGURIDAD_DE_LA_INFORMACIÓN_REQUISITOS.

[15] S. M. T. Toapanta, N. M. M. Maldonado, L. E. M. Gallegos, and M. P. Solis, “Security prototype to determine critical information and improve the management of a public organization,” *2020 Asia Conf. Comput. Commun. ACCC 2020*, pp. 82–90, 2020, doi: 10.1109/ACCC51160.2020.9347902.

[16] S. Patino, E. F. Solis, S. G. Yoo, and R. Arroyo, “ICT Risk Management Methodology Proposal for Governmental Entities Based on ISO/IEC 27005,” *2018 5th Int. Conf. eDemocracy eGovernment, ICEDEG 2018*, pp. 75–82, 2018, doi: 10.1109/ICEDEG.2018.8372361.

[17] E. Kowask Bezerra, F. Alcántara Lima, A. C. Motta, and J. D. B. Piccolini, “Gestión del riesgo de las TI NTC 27005,” *Red Nac. Investig. y Educ. del Ecuador REDCEDIA*, p. 217, 2014.

ANEXOS

Anexo 1. Entrevista

1. ¿Cuáles son los procesos que emplean en este departamento para gestionar y almacenar la información?
2. ¿Qué activos usan en cada proceso?
3. ¿Quién es el propietario de “x” activo?
4. ¿Quién es el responsable de “x” activo?
5. ¿Qué información almacena “x” activo?
6. ¿Qué información genera “x” activo?
7. ¿Qué usuarios tienen acceso a la información?
    a) *Estudiante*
    b) *Profesor*
    c) *Personal administrativo*
    d) *Prospectos*
    e) *Exestudiantes*
    f) *Ciudadanía*
8. ¿Cómo categorizaría este activo?
    a) *Información sensible*
    b) *Información critica*
    c) *Información distribuible*

Confidencialidad

9. ¿Existe un método para controlar el acceso a este activo?
10. ¿En una escala del 1 al 5 cómo calificaría la confidencialidad de este activo?

Integridad

11. ¿Qué personas pueden modificar este activo?
12. ¿Existe un control para evitar que cualquier persona pueda modificar este activo?
13. ¿En una escala del 1 al 5 cómo calificaría la integridad de este activo?

Disponibilidad

14. ¿La información a este activo es accesible todo el tiempo para los usuarios que tienen acceso?
15. ¿En una escala del 1 al 5 cómo calificaría la integridad de este activo?

Anexo 2. Tabla para inventario de activos

Tabla 4. Primera parte del inventario de activos

Código TI	**Activo**	**Propietario**	**Descripción del activo**	**Tipo de activo**	**Área/proceso**	**Ubicación de activo**	**Medio de conservación físico y/o digital**	**¿Hay datos sensibles?**	**¿Hay datos personales?**

Tabla 5. Segunda parte del inventario de activos

Responsable	**Usuarios**							**Correlación**	**Clasificación por confidencialidad**			
Funcional	Informático	Estudiante	Profesor	Personal administrativo	Prospectos	Exestudiante	Ciudadanía		Pública reservada	Pública clasificada	Pública	No aplica

Anexo 3. Tabla de evaluación del nivel de impacto de los activos

A continuación, se presenta en la tabla un listado de todos los activos de información indicando el valor de confidencialidad, integridad, disponibilidad y el nivel de impacto del riesgo para la seguridad de la información que tendría en la universidad.

Tabla 6 Evaluación del nivel de impacto

Código TI	Activo	Confidencialidad	Integridad	Disponibilidad	Nivel de impacto
A001	Página web	2	3	5	10
A002	Base de datos página web	4	5	5	14
A003	Aula virtual 2020	4	5	5	14
A004	Base de datos aula virtual 2020	4	4	4	12
A005	Aula virtual 2021	4	5	5	14
A006	Base de datos aula virtual 2021	4	4	4	12
A007	Aula virtual 2022	4	5	5	14
A008	Base de datos aula virtual 2022	4	4	4	12
A009	Moodle identificación	4	5	5	14
A010	Base de datos Moodle identificación	4	4	4	12
A011	Moodle cursos	4	4	4	12
A012	Base de datos Moodle cursos	4	4	4	12
A013	Intranet	4	5	5	14
A014	Base de datos intranet	4	4	4	12
A015	Revista	2	2	2	6
A016	Base de datos revista	4	4	4	12
A017	CFC (sistema para formación continua)	5	4	5	14
A018	Base de datos CFC (sistema para formación continua)	5	4	5	14
A019	Avales académicos	5	5	5	15
A020	Base de datos matriz de avales académicos	5	5	5	15
A021	Informe de avales académicos	5	5	5	15
A022	Eventos académicos	5	5	5	15
A023	Base de datos eventos académicos	5	5	5	15
A024	Informe de eventos	5	5	5	15
A025	Ofertas académicas	5	5	5	15

A026	Base de datos de prospectos o prototipos	5	5	5	15
A027	Informe de prospectos o prototipos	5	5	5	15
A028	Informe de inscritos	4	5	5	14
A029	Idiomas	5	5	5	15
A030	Informe de inscritos	5	5	5	15
A031	Nivelación	5	5	5	15
A032	Informe de inscritos	5	5	5	15
A033	Moodle admisiones	5	5	5	15
A034	Base de datos Moodle admisiones	5	5	5	15
A035	GLPI (sistema de soporte)	4	5	5	14
A036	Base de datos GLPI (sistema de soporte)	4	5	5	14
A037	OJS	4	4	5	13
A038	Extensión telefónica	5	5	5	15
A039	Base de datos identificación	5	5	5	15
A040	Firewall	5	5	5	15
A041	Base de datos firewall	5	5	5	15
A042	Banner estudiante	4	4	5	13
A043	Base de datos banner estudiante	4	4	5	13
A044	Banner docente	4	4	5	13
A045	Base de datos banner docente	4	4	5	13
A046	Proceso de solicitud de informes	4	4	5	13
A047	Excel para control de informes	5	4	5	14
A048	Base de datos en la red	5	5	5	15
A049	Informes de gestión semestral	4	4	4	12
A050	Homologaciones	2	2	2	6
A051	KOHA biblioteca	3	3	3	9
A052	Informes del sistema KOHA	3	3	3	9
A053	Repositorio de tesis	3	3	3	9
A054	Sistema KARMEC	3	2	5	10

A055	Base de datos sistema KARMEC	3	2	5	10
A056	Reporte en Excel	3	3	5	11
A057	Historias clínicas	5	5	5	15
A058	Recetas	3	2	5	10
A059	Interconsultas	3	2	5	10
A060	Imágenes	3	2	5	10
A061	Archivos de pacientes	4	4	4	12
A062	Certificados médicos	3	2	5	10
A063	Pedidos de laboratorios	3	2	5	10
A064	Banner	5	5	3,5	13.5
A065	Argos	5	5	5	15
A066	Archivo	4	4	4	12

Anexo 4. Declaración de aplicabilidad

Tabla 7. Declaración de aplicabilidad

ID CONTROL	CONTROL	APLICA	SE IMPLEMENTA
A.5	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN		
A.5.1	Directrices de gestión de la seguridad de la información		
A.5.1.1	Políticas para la seguridad de la información	SI	NO
A.5.1.2	Revisión de las políticas para la seguridad de la información	SI	NO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		
A.6.1	Organización Interna		
A.6.1.1	Roles y responsabilidades para la seguridad de la información	SI	NO
A.6.1.2	Segregación de tareas	SI	NO
A.6.1.3	Contacto con las autoridades	SI	NO
A.6.1.4	Contacto con grupos de interés especial	SI	NO
A.6.1.5	Seguridad de la información en la gestión de proyectos	SI	NO
A.6.2	Los dispositivos móviles y el teletrabajo		
A.6.2.1	Políticas de dispositivos móviles	SI	NO
A.6.2.2	Teletrabajo	SI	NO
A.7	SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS		

A.7.1	Antes del empleo		
A.7.1.1	Investigación de antecedentes	SI	SI
A.7.1.2	Términos y condiciones del empleo	SI	SI
A.7.2	Durante el empleo		
A.7.2.1	Responsabilidades de gestión	SI	NO
A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	SI	NO
A.7.2.3	Proceso disciplinario	SI	SI
A.7.3	Finalización del empleo o cambio en el puesto de trabajo		
A.7.3.1	Responsabilidades ante la finalización o cambio	SI	SI
A.8	GESTIÓN DE ACTIVOS		
A.8.1	Responsabilidad sobre los activos		
A.8.1.1	Inventario de activos	SI	NO
A.8.1.2	Propiedad de los activos	SI	NO
A.8.1.3	Uso aceptable de los activos	SI	NO
A.8.1.4	Devolución de activos	SI	NO
A.8.2	Clasificación de la información		
A.8.2.1	Clasificación de la información	SI	NO
A.8.2.2	Etiquetado de la información	SI	NO
A.8.2.3	Manipulado de la información	SI	NO
A.8.3	Manipulación de los soportes		
A.8.3.1	Gestión de soportes extraíbles	SI	NO
A.8.3.2	Eliminación de soportes	SI	NO
A.8.3.3	Soportes físicos en tránsito	SI	NO
A.9	CONTROL DE ACCESO		
A.9.1	Requisitos de negocio para el control de acceso		
A.9.1.1	Política de control de acceso	SI	NO
A.9.1.2	Acceso a las redes y a los servicios de red	SI	SI
A.9.2	Gestión de acceso de usuario		
A.9.2.1	Registro y baja de usuario	NO	NO
A.9.2.2	Provisión de acceso de usuario	NO	NO
A.9.2.3	Gestión de privilegios de acceso	SI	SI
A.9.2.4	Gestión de la información secreta de autenticación de los usuarios	SI	SI
A.9.2.5	Revisión de los derechos de acceso de usuario	SI	NO
A.9.2.6	Retirada o reasignación de los derechos de acceso	SI	
A.9.3	Responsabilidades del usuario		
A.9.3.1	Uso de la información secreta de autenticación	SI	SI
A.9.4	Control de acceso a sistemas y aplicaciones		

A.9.4.1	Restricción del acceso a la información	SI	SI
A.9.4.2	Procedimientos seguros de inicio de sesión	SI	SI
A.9.4.3	Sistema de gestión de contraseñas	SI	SI
A.9.4.4	Uso de utilidades con privilegios del sistema	SI	NO
A.9.4.5	Control de acceso al código fuente de los programas	SI	SI
A.10	CRIPTOGRAFÍA		
A.10.1	Controles criptográficos		
A.10.1.1	Política de uso de los controles criptográficos	NO	NO
A.10.1.2	Gestión de claves	NO	NO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO		
A.11.1	Áreas seguras		
A.11.1.1	Perímetro de seguridad física	SI	SI
A.11.1.2	Controles físicos de entrada	SI	NO
A.11.1.3	Seguridad de oficinas, despachos y recursos	SI	SI
A.11.1.4	Protección contra las amenazas externas y ambientales	SI	NO
A.11.1.5	El trabajo en áreas seguras	NO	NO
A.11.1.6	Áreas de carga y descarga	NO	NO
A.11.2	Seguridad de los equipos		
A.11.2.1	Emplazamiento y protección de equipos	SI	NO
A.11.2.2	Instalaciones de suministro	SI	SI
A.11.2.3	Seguridad del cableado	SI	SI
A.11.2.4	Mantenimiento de los equipos	SI	SI
A.11.2.5	Retirada de materiales propiedad de la empresa	SI	NO
A.11.2.6	Seguridad de los equipos fuera de las instalaciones	SI	SI
A.11.2.7	Reutilización o eliminación segura de equipos	SI	SI
11.2.8	Equipo de usuario desatendido	SI	SI
11.2.9	Política de puesto de trabajo despejado y pantalla limpia	SI	NO
12	SEGURIDAD DE LAS OPERACIONES		
12.1	Procedimientos y responsabilidades operacionales		
12.1.1	Documentación de procedimientos de las operaciones	SI	NO
12.1.2	Gestión de cambios	SI	SI
12.1.3	Gestión de capacidades	SI	NO
12.1.4	Separación de los recursos de desarrollo, prueba y operación	NO	NO
12.2	Protección contra el software malicioso (malware)		
12.2.1	Controles contra el código malicioso	SI	SI

12.3	Copias de seguridad		
12.3.1	Copias de seguridad de la información	SI	SI
12.4	Registros y supervisión		
12.4.1	Registro de eventos	SI	NO
12.4.2	Protección de la información del registro	SI	NO
12.4.3	Registros de administración y operación	SI	NO
12.4.4	Sincronización del reloj	SI	SI
12.5	Control del software en explotación		
12.5.1	Instalación del software en explotación	SI	SI
12.6	Gestión de la vulnerabilidad técnica		
12.6.1	Gestión de las vulnerabilidades técnicas	SI	NO
12.6.2	Restricción en la instalación de software	SI	SI
12.7	Consideraciones sobre la auditoria de sistemas de información		
12.7.1	Controles de auditoría de sistemas de información	SI	NO
13	SEGURIDAD DE LAS COMUNICACIONES		
13.1	Gestión de la seguridad de redes		
13.1.1	Controles de red	SI	SI
13.1.2	Seguridad de los servicios de red	SI	SI
13.1.3	Segregación en redes	SI	SI
13.2	Intercambio de información		
13.2.1	Políticas y procedimientos de intercambio de información	SI	NO
13.2.2	Acuerdos de intercambio de información	SI	NO
13.2.3	Mensajería electrónica	SI	NO
13.2.4	Acuerdos de confidencialidad o no revelación	SI	NO
14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN		
14.1	Requisitos de seguridad en los sistemas de información		
14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	SI	SI
14.1.2	Asegurar los servicios de aplicaciones en redes públicas	NO	NO
14.1.3	Protección de las transacciones de servicios de aplicaciones	SI	NO
14.2	Seguridad en el desarrollo y en los procesos de soporte		
14.2.1	Política de desarrollo seguro	SI	NO
14.2.2	Procedimiento de control de cambios en sistemas	SI	NO
14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	SI	SI

14.2.4	Restricciones a los cambios en los paquetes de software	SI	NO
14.2.5	Principios de ingeniería de sistemas seguros	SI	NO
14.2.6	Entorno de desarrollo seguro	SI	NO
14.2.7	Externalización del desarrollo de software	SI	SI
14.2.8	Pruebas funcionales de seguridad de sistemas	SI	SI
14.2.9	Pruebas de aceptación de sistemas	SI	SI
14.3	Datos de prueba		
14.3.1	Protección de los datos de prueba	SI	SI
15	RELACIÓN CON PROVEEDORES		
15.1	Seguridad en las relaciones con proveedores		
15.1.1	Política de seguridad de la información en las relaciones con los proveedores	SI	NO
15.1.2	Requisitos de seguridad en contratos con terceros	SI	SI
15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	SI	NO
15.2	Gestión de la provisión de servicios del proveedor		
15.2.1	Control y revisión de la provisión de servicios del proveedor	SI	SI
15.2.2	Gestión de cambios en la provisión del servicio del proveedor	SI	NO
16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN		
16.1	Gestión de incidentes de seguridad de la información y mejoras		
16.1.1	Responsabilidades y procedimientos	SI	NO
16.1.2	Notificación de los eventos de seguridad de la información	SI	SI
16.1.3	Notificación de puntos débiles de la seguridad	SI	SI
16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	SI	NO
16.1.5	Respuesta a incidentes de seguridad de la información	SI	NO
16.1.6	Aprendizaje de los incidentes de seguridad de la información	SI	NO
16.1.7	Recopilación de evidencias	SI	NO
17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO		
17.1	Continuidad de la seguridad de la información		
17.1.1	Planificación de la continuidad de la seguridad de la información	SI	NO

17.1.2	Implementar la continuidad de la seguridad de la información	SI	NO
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	SI	NO
17.2	Redundancias		
17.2.1	Disponibilidad de los recursos de tratamiento de la información	SI	NO
18	CUMPLIMIENTO		
18.1	Cumplimiento de los requisitos legales y contractuales		
18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	SI	SI
18.1.2	Derechos de propiedad intelectual (DPI)	SI	NO
18.1.3	Protección de los registros de la organización	SI	NO
18.1.4	Protección y privacidad de la información de carácter personal	SI	NO
18.1.5	Regulación de los controles criptográficos	SI	NO
18.2	Revisiones de la seguridad de la información		
18.2.1	Revisión independiente de la seguridad de la información	SI	NO
18.2.2	Cumplimiento de las políticas y normas de seguridad	SI	NO
18.2.3	Comprobación del cumplimiento técnico	SI	NO