UNIVERSIDAD TECNOLÓGICA ISRAEL
ESCUELA DE POSTGRADOS

MAESTRÍA EN TELEMÁTICA, MENCIÓN: CALIDAD EN EL SERVICIO

(Aprobado por: RPC-SO-19-No.300-2016-CES)

TRABAJO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER

Título:
Diseño de un Modelo de Gestión de Seguridad de la Información para la Universidad Iberoamericana del Ecuador.
Autor/a:
Ana Cecilia Quintana Arroyo
Tutor/a:
Mg. Henry Rodrigo Vivanco Herrera

Quito-Ecuador 2019

CERTIFICADO DE RESPONSABILIDAD

Yo, Mg. Henry Vivanco, certifico que la Ing. Ana Cecilia Quintana Arroyo con C. C. 1708670284 realizó la presente tesis con el título: "Diseño de un modelo de gestión de seguridad de la información para la Universidad Iberoamericana del Ecuador", y que es autor intelectual de la misma, que es original, auténtica y personal.

Quito, Febrero 2019

_____

Mg. Henry Vivanco

CERTIFICADO DE AUTORÍA

El presente trabajo titulación con título: “Diseño de un modelo de gestión de seguridad de la información para la Universidad Iberoamericana del Ecuador”, ha sido desarrollado por la Ing. Ana Cecilia Quintana con C.C. 1708670284 que posee los derechos de autoría y responsabilidad, restringiéndose la copia o utilización de la información de esta tesis sin previa autorización.

_____

Ing. Ana C. Quintana A.
C. C. 1708670284

DEDICATORIA

A mi familia, por su apoyo incondicional y perseverante que me permitió mantener una dedicación constante en la elaboración de este trabajo.

AGRADECIMIENTO

A mi Dios, por ser la fuente de fortaleza para lograr este objetivo.

A la Universidad Iberoamericana por su apoyo y confianza, que me han permitido conseguir esta meta profesional.

A todos los profesores que contribuyeron en el presente trabajo.

RESUMEN

La seguridad de la información juega un papel fundamental en el funcionamiento diario de las organizaciones de cualquier tipo entre ellas las instituciones de educación superior que por su dedicación al servicio de la sociedad deben proteger aún más la información que manejan, las normas ISO/IEC 27001 se han constituido en marco de referencia en cuanto a la seguridad de la información, dando guías prácticas para gestionarla de manera sistemática y confiable. Esta norma en conjunto con la ISO/IEC 27005 permite tener una idea clara de las amenazas a las que la información se expone especialmente en la actualidad en la que todo el mundo está interconectado. El Sistema de Gestión de Seguridad de la Información permite proteger la información y garantiza el funcionamiento continuo de los sistemas de información institucionales.

En la presente investigación se plantea un modelo de un Sistema de Gestión de Seguridad de la Información para la Universidad Iberoamericana del Ecuador, a través de la adopción de la norma ISO/IEC 27001 que define los requisitos para los Sistemas de Gestión de la Información y de la norma ISO/IEC 27005 que brinda lineamientos generales para crear una metodología de gestión de riesgos. Se inicia con un análisis de la situación actual de la Institución y se especifican los pasos necesarios a seguir para la implementación del modelo.

Palabras claves: Seguridad de la información, SGSI, normas ISO, riesgos, 27001

ABSTRACT

The security of information plays a fundamental role in the daily functioning of organizations of any type, including higher education institutions that, because of their dedication to the service of society, they must protect even more the information they handle. The ISO/IEC 27001 standards have become a reference framework for information security, providing practical guidelines to manage it in a systematic and reliable manner. This standard, along with ISO/IEC 27005, allows us to have a clear idea of the threats, information is exposed to, especially, in times like these where everyone is interconnected. The Information Security Management System allows the protection of information and guarantees the continuity of the institutional information systems.

In the present investigation, a model of an Information Security Management System is proposed for Universidad Iberoamericana del Ecuador through the adoption of the ISO/IEC 27001 standard that specifies the requirements for Information Management Systems, and the ISO/IEC 27005 standard that provides general guidelines for creating a risk management methodology. An analysis of the current situation of the Institution is made, and the necessary steps to follow for the implementation of the model are specified.

Keywords: Information security, ISMS, ISO standards, risks, 27001

ÍNDICE DE CONTENIDOS

DEDICATORIA III
AGRADECIMIENTO IV
RESUMEN V
ABSTRACT VI
ÍNDICE DE CONTENIDOS VII
ÍNDICE DE FIGURAS X
ÍNDICE DE TABLAS XI
ÍNDICE DE ANEXOS XII
INTRODUCCIÓN 1
PROBLEMA 1
OBJETIVO GENERAL: 3
OBJETIVOS ESPECÍFICOS: 3
HIPÓTESIS DE INVESTIGACIÓN 3
JUSTIFICACIÓN 3
CAPÍTULO I: MARCO TEÓRICO 5
1.1. Seguridad de la Información 5
1.2. Sistema de Gestión de Seguridad de la Información 7
1.3. Normas y estándares que rigen la Seguridad de la Información 9
1.3.1. Norma BS7799-2 9
1.3.2. O-ISM3 9
1.3.3. Serie ISO/IEC 27000 10
1.3.3.1. ISO/IEC 27000:2018 11
1.3.3.2. ISO/IEC 27001:2013 11
1.3.3.3. ISO/IEC 27002:2017 13
1.4. Metodología de la Gestión de Riesgos 14
1.4.1. MAGERIT 16
1.4.2. OCTAVE 16
1.4.3. ISO 31010 17

1.4.4. RISK IT 17
1.1.1. ISO/IEC 27005 17
CAPÍTULO II: MARCO METODOLÓGICO 20
2.1. Enfoque metodológico de la investigación. 20
2.2. Población, unidades de estudio y muestra. 20
2.2.1. Población 20
2.2.2. Muestra 20
2.3. Técnica de recolección de datos 21
2.3.1. Encuestas 21
2.3.2. Entrevistas 22
2.3.3. Observación directa 22
2.4. Formas de procesamiento de la información 22
2.5. Situación Actual 22
2.5.1. Estado de madurez respecto a la norma ISO/IEC27001 30
2.6. Metodología seleccionada 33
CAPÍTULO III: PROPUESTA 37
3.1. Fundamentos de la propuesta 37
3.2. Fase I Contexto de la organización 38
3.2.1. Misión 38
3.2.2. Objetivos estratégicos 38
3.2.4. Estructura de la Universidad 39
3.3. Fase II Liderazgo 41
3.3.1. Alcance 41
3.3.2. Objetivos del SGSI 42
3.3.3. Política General de Seguridad de la Información. 43
3.3.4. Definición de roles y responsabilidades 49
3.4. Fase III Planificación: Gestión de riesgos de la información 50
3.4.1. Metodología de la gestión de riesgos de la seguridad de la información 51
3.4.2. Inventario de activos de información 51

3.4.3. Valoración de Activos 56
3.4.4. Determinar amenazas y vulnerabilidades de los activos 60
3.4.5. Tratamiento del riesgo 68
3.5. Fase IV Documentación del SGSI 69
3.5.1. Declaración de Aplicabilidad 69
3.5.2. Plan de tratamiento del riesgo 78
3.6. Fase V Plan de Implementación del SGSI 80
3.6.1. Plan de Implementación del SGSI 80
CONCLUSIONES 82
RECOMENDACIONES 84
BIBLIOGRAFÍA 85
ANEXOS 87

ÍNDICE DE FIGURAS

Figura 1. Estado Seguridad Información Universidades – Ecuador 2
Figura 2. Características de Seguridad 5
Figura 3. Ciclo de mejora continua 8
Figura 4. Estructura de la ISO/IEC 27001 12
Figura 5. Esquema de la gestión de riesgos 15
Figura 6. Ciclo de la gestión de riesgos 18
Figura 7. Seguridad de la Información 23
Figura 8. Porcentajes totales 24
Figura 9. Política de Seguridad de la información 25
Figura 10. Capacitación sobre Seguridad de la Información 25
Figura 11. Sabe qué hacer en un incidente de seguridad 26
Figura 12. Generar cultura de Seguridad de la Información 27
Figura 13 Identificada información que utiliza 27
Figura 14 ¿Procesos definidos claramente? 28
Figura 15 Tiempo de retención de la información 29
Figura 16 Procedimiento para destruir información 29
Figura 17. Grado de madurez respecto al SGSI 33
Figura 18. Pasos del SGSI de acuerdo con el ciclo de calidad y la ISO/IEC 27001 34
Figura 19. Diagrama de Bloques de la Metodología 35
Figura 20. Organigrama de la Universidad 40

ÍNDICE DE TABLAS

Tabla 1. Normas ISO 27000 11
Tabla 2. Estructura de la norma ISO/IEC 27001 12
Tabla 3. Dominios de Seguridad 13
Tabla 4. Pasos de la Gestión de Riesgo 18
Tabla 5. Tipos de activos de información [24] 18
Tabla 6. Distribución de población 20
Tabla 7. Distribución de personal en las Direcciones 21
Tabla 8. Estado de madurez SGSI 30
Tabla 9. Fases del diseño de SGSI 36
Tabla 10. Roles administrativos para el SGSI 41
Tabla 11. Descripción de Procesos 42
Tabla 12. Inventario de Activos de Información 52
Tabla 13. Criterios de impacto 56
Tabla 14. Valoración de activos 57
Tabla 15. Ejemplos de Amenazas 60
Tabla 16. Probabilidad que ocurra la amenaza 61
Tabla 17. Impacto de ocurrencia de un riesgo 62
Tabla 18. Valoración del riesgo en los activos de información 62
Tabla 19. Decisiones de tratamiento del riesgo 69
Tabla 20. Declaración de aplicabilidad 70
Tabla 21. Plan de Tratamiento de riesgos 78
Tabla 22. Plan de implementación del SGSI 80

ÍNDICE DE ANEXOS

Anexo 1. Modelo de Cuestionario

Anexo 2. Modelo de Entrevista

Anexo 3. Lista de amenazas y vulnerabilidades

Anexo 4. Carta de Apoyo Institucional

INTRODUCCIÓN

Los estándares de aceptación general, como son las normas ISO 27001, son un referente confiable para la implantación, optimización y administración de procesos dentro de una organización.

En el caso particular de la Universidad Iberoamericana del Ecuador, al momento no dispone de procesos de seguridad de la información, tampoco un modelo de gestión que permita asegurar la información que maneja, siendo esta muy sensible dado que con los sistemas de información se maneja tanto las notas como la trayectoria e información personal de los estudiantes y docentes, así como información financiera y de control.

La adopción de un modelo de gestión de la seguridad de la información permitirá proteger la información generada y contenida en cualquier medio de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información académicos, financieros, de talento humano y tecnológicos, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de negocio. Considerando que la información es un recurso muy importante y estratégico para cualquier organización ésta debe ser debidamente protegida.

La metodología a utilizar se basará en las siguientes fases:

- Un planteamiento teórico sobre las normas técnicas ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27005, para la definición y diseño de un Sistema de Gestión de Seguridad de la Información (SGSI), los controles para la seguridad de la información y la metodología de riesgos.

- Análisis de la situación actual de la seguridad de la información en la Universidad Iberoamericana.

- Desarrollo del modelo de gestión de la seguridad de la información.

PROBLEMA

La seguridad de la Información ha cobrado una mayor relevancia en los últimos tiempos, debido al aumento de incidentes de seguridad que se han presentado en diferentes organizaciones a nivel mundial y que han puesto en riesgo información importante para las

mismas, especialmente en aquellas que no cuentan con procesos de gestión de estos incidentes. A nivel mundial la norma ISO/IEC 27001 se ha convertido en la norma más utilizada para la gestión de la seguridad de la información.

En el Ecuador los institutos de educación superior cada vez toman más conciencia de la necesidad de contar con mecanismos que ayuden a garantizar su funcionamiento y mantengan seguros sus sistemas de información, en la Figura 1 se puede observar el estado de la seguridad de la información en las universidades ecuatorianas.

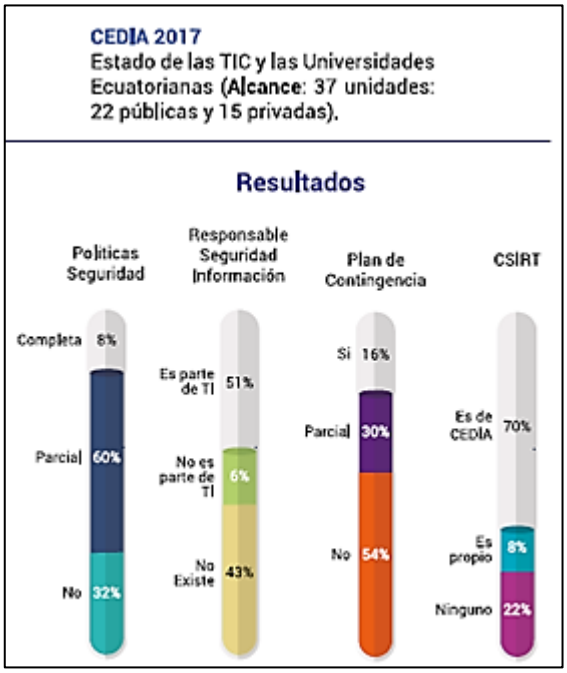


Figura 1. Estado Seguridad Información Universidades – Ecuador
Fuente: (MINTEL, 2018)

Como se había expuesto la información se puede considerar como uno de los activos más importantes con los que cuenta la institución y tiene un valor estratégico para la misma, por ello es también muy vulnerable a las amenazas, por lo que debe protegerse adecuadamente, en la actualidad la Universidad Iberoamericana del Ecuador no cuenta con procesos de seguridad de la información definidos, ni tampoco con un modelo de gestión que permita asegurar la información que maneja. Los procesos de seguridad no se encuentran debidamente documentados ni socializados con la comunidad universitaria. Adicionalmente esta falta de estructura en los procesos hace que no se asegure la información que se maneja en los diferentes puestos de trabajo y puede provocar pérdida de información o que ésta no sea confiable ni esté disponible cuando se la requiera.

La adopción de un Sistema de Gestión de Seguridad de la Información permitirá proteger la información generada y contenida en cualquier medio de una amplia gama de amenazas, a fin de garantizar la continuidad de los Sistemas de Información, tanto Académicos y Financieros, minimizando los riesgos de daño y asegurando el cumplimiento de sus objetivos.

OBJETIVO GENERAL:

Diseñar un Modelo de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001, para la Universidad Iberoamericana del Ecuador.

OBJETIVOS ESPECÍFICOS:

- Investigar las normas internacionales para la implementación de un Sistema de Seguridad de la Información en la Universidad Iberoamericana del Ecuador (UNIB.E).
- Determinar la situación actual de la seguridad de la información en la UNIB.E.
- Analizar la metodología de gestión de riegos de seguridad de la información para la UNIB.E.
- Realizar el diseño del modelo de Gestión de Seguridad de la Información, basado en la familia de normas ISO 27001.

HIPÓTESIS DE INVESTIGACIÓN

La hipótesis de la investigación es:

- ¿El SGSI en la Universidad Iberoamericana del Ecuador asegurará la confiabilidad, disponibilidad e integridad de la información más sensible de la Institución?

JUSTIFICACIÓN

Los procesos críticos de las instituciones de educación superior al igual que de la mayoría de organizaciones están soportados por la información que en la actualidad viene a constituirse en su activo más importante, sin embargo, la seguridad de dicha información hoy en día es cada vez más difícil de garantizar, debido al uso intensivo de la tecnología y del Internet, lo que hace que estén expuestos a diversa clase de amenazas tanto internas como externas, que afectan a la integridad, confiabilidad y disponibilidad de dicha información.

Para minimizar dichas amenazas es recomendable instaurar un sistema que gestione la seguridad de la información, estos sistemas permiten una reacción oportuna y eficaz frente a los diversos eventos de seguridad que puedan presentarse.

Al no contar con un Sistema de Gestión de Seguridad de la Información en la Universidad Iberoamericana del Ecuador (UNIB.E), ha incidido en la falta de normas y procedimientos que aseguren la calidad de la información y minimicen los daños a la infraestructura tecnológica de la Universidad por lo que puede perderse información valiosa para su funcionamiento normal y para los procesos de acreditación que los organismos reguladores de la educación superior están llevando a cabo, esta pérdida de información puede generar un retraso en la en la entrega de información solicitada por los organismos de control del Ecuador.

CAPÍTULO I: MARCO TEÓRICO

1.1. Seguridad de la Información

Actualmente para la mayoría de empresas o instituciones, la información es un instrumento fundamental para su funcionamiento, y el que necesita de una mayor protección ya que el uso intensivo del Internet y la tecnología ha originado que las amenazas que aprovechan las vulnerabilidades de las organizaciones hayan aumentado, ocasionando que se pierdan alguna de las características que la seguridad de la información debe preservar es decir la disponibilidad, la integridad y la confidencialidad de ésta (Areitio, 2008). Dichas características contribuyen a lograr la seguridad de la información y están estrechamente relacionadas entre sí, como puede observarse en la Figura 2.

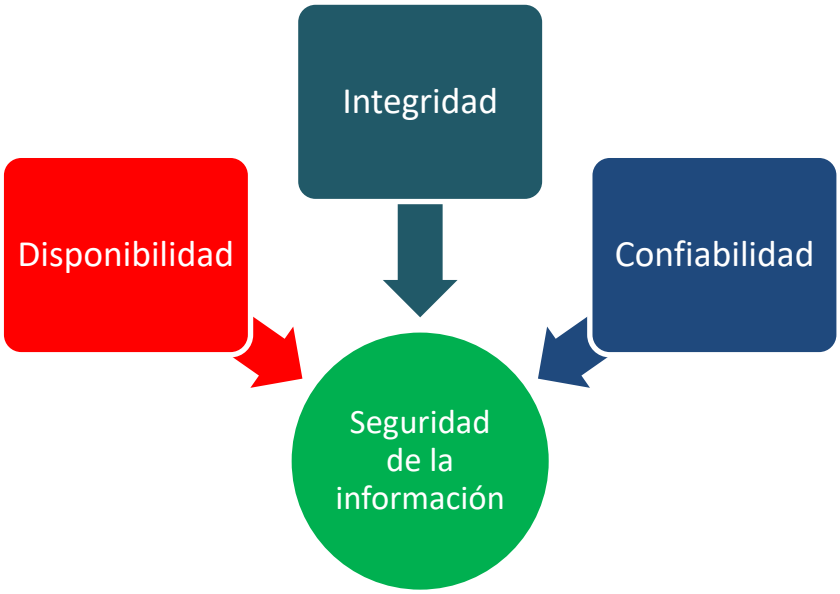


Figura 2. Características de Seguridad
Fuente: Adaptado de (Gómez Á. , 2014)

Las características de seguridad nombradas anteriormente pueden conceptualizarse según la norma (ISO 27000, 2018), de la siguiente manera:

- Confidencialidad: es la imposibilidad de que las personas, o procesos no autorizados puedan acceder a la información.
- Integridad: es la capacidad de garantizar la exactitud de la información a la que se accede.

- Disponibilidad: es el acceso y utilización de la información en el momento que ésta es requerida.

Las instituciones de educación superior como cualquier otra organización dependen también de la información para alcanzar sus objetivos estratégicos con calidad y excelencia, de manera que puedan cumplir con las expectativas tanto de sus clientes que serían los alumnos, como de proveedores y organismos de control del estado, especialmente en los procesos continuos de control y evaluación por parte de estos.

De acuerdo con la norma ISO 27000 (2018), la información es considerada un activo, incluso mucho más significativo que otros por su importancia estratégica, por esta razón debe ser protegida de cualquier riesgo. La información no necesariamente está almacenada de forma digital, sino que en general se considera que puede estar también en forma física es decir impresa e inclusive el conocimiento que tienen las personas que realizan un trabajo específico.

En general como lo expresa Carpentier (2016) la seguridad de la información tiene como objetivos primordiales proteger la confidencialidad, integridad y disponibilidad de la misma, esto ayuda a que:

- La información sensible o confidencial no se divulgue de forma no autorizada o se vea comprometida.
- La información crítica no sea modificada o alterada accidental o intencionalmente.
- No se pierda información importante sin posibilidad de recuperación.
- La información esté disponible cuando sea necesaria.

Hay que recalcar que cuando se habla de seguridad de la información no se hace referencia únicamente a la protección de las TIC, sino que el concepto es mucho más amplio ya se extiende a la protección de todos los activos de información de la organización estén en cualquier medio o formato (Gómez & Fernández, 2018).

La protección de la información es esencial para que las organizaciones, puesto que permite cumplir con la normativa legal y mantener también una buena reputación de cara a sus clientes o competidores, cada organización debe establecer objetivos y políticas de

seguridad, que permitan un trabajo eficiente, esto puede lograrse de una manera planificada si se implementa un sistema de gestión de seguridad (Carpentier, 2016).

1.2. Sistema de Gestión de Seguridad de la Información

Como anteriormente se había indicado, uno de los métodos a disposición de las organizaciones para el manejo de la seguridad es el establecimiento de un Sistema de Gestión de Seguridad de la Información (SGSI), que de acuerdo con Giménez (2014), son las acciones o pasos que permiten establecer, implementar, mantener y mejorar continuamente la seguridad de la información, basándose en una determinación de los riesgos que se pueden presentar en la organización. Como expresa la norma ISO 27000 (2018), el SGSI es por lo tanto un proceso sistemático que necesita el apoyo de las autoridades y de toda la organización.

Este Sistema de Gestión debe procurar que la organización alcance sus objetivos de negocio, protegiendo los activos de información, mediante políticas y procedimientos que brinden directrices aplicables en toda la organización, por lo que el SGSI es básicamente un marco de referencia de seguridad (ISO 27000, 2018).

ISO 27000 en español (s.f.), indica que un SGSI permite a la organización: cumplir con los requisitos u objetivos de seguridad de la información que la organización quiera alcanzar, mejorando la manera en la que se maneja la información, y cumpliendo con reglamentos, disposiciones o leyes establecidas por los organismos de control.

El SGSI debe determinar los diferentes riesgos a los que podría estar expuesta la información para determinar las políticas, procedimientos, controles o métodos para minimizar estos riesgos, todos esto procedimientos deben documentarse y socializarse; según Gómez y Fernández (2018), un SGSI se organiza en las cuatro fases típicas del ciclo de Deming o ciclo de mejora continua, es decir: planear, hacer, verificar y actuar cuya relación se indica en la Figura 3.

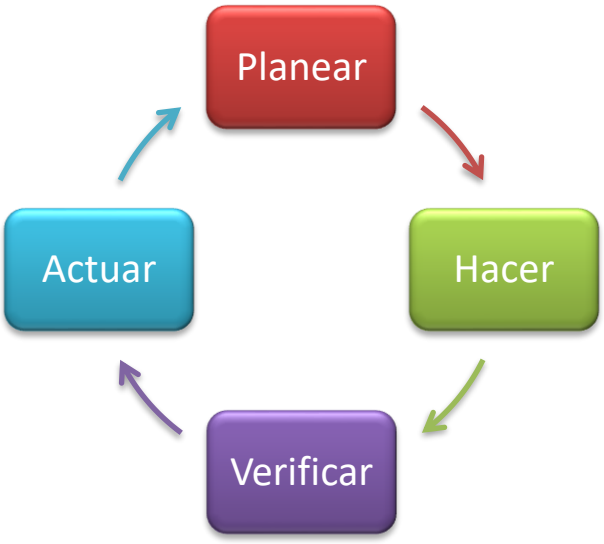


Figura 3. Ciclo de mejora continua
Fuente: adaptado de (Gómez & Fernández, 2018)

Como establece Pallas (2009), un Sistema de Gestión de Seguridad de la Información debe contemplar entre otras las siguientes tareas:

- Establecer un alcance para el SGSI.
- Determinar unos objetivos de seguridad de la información que sean aplicables a la organización.
- Considerar requisitos tanto legales, administrativos o de otro tipo que influyan en la seguridad de la información.
- Realizar la gestión de riesgos para determinar las amenazas y vulnerabilidades que puedan poner afectar a los activos de información.
- Contar con el respaldo de las autoridades de la organización.

Los beneficios que se obtienen al implementar un SGSI de acuerdo con la norma ISO 27000 (2018) son:

- Contar con un marco normativo ajustado a las necesidades de la organización.
- Permitir una gestión de la seguridad de la información con el apoyo e involucramiento de toda la organización.

- Fomentar en la organización buenas prácticas de seguridad de la información internacionalmente aceptadas.
- Crear un compromiso de mantener la seguridad de la información, en el trabajo cotidiano.
- Dar una buena imagen y fomentar la confianza de clientes, usuarios, proveedores u otro grupo con interés en la organización
- Mejorar el retorno de las inversiones que se realicen para implementar la seguridad de la información.

1.3. Normas y estándares que rigen la Seguridad de la Información

1.3.1. Norma BS7799-2

La norma británica BS7799-2 establece un marco de referencia para diseñar y administrar un Sistema de Gestión de Seguridad (SGSI), brinda recomendaciones para la gestión de la seguridad de la información y de la misma manera presenta los controles necesarios que permitan garantizar la seguridad de la información, (Rifan, 2004).

El objetivo de la norma BS7799 es proteger la información de las amenazas y vulnerabilidades que pueden afectarle y garantizar la continuidad del negocio, da importancia a los mecanismos que ayuden a mejorar la seguridad de la información. Sus objetivos son: proporcionar una guía de mejores prácticas de seguridad de la información, ayudar a identificar fortalezas y debilidades en los procesos de gestión de seguridad de la información y planear acciones de mejora que apoyen el logro de los objetivos de la organización (Haiwen & Graham, 2000).

BS 7799 es la norma en la que se basa la ISO/IEC27701, que es la que en la actualidad está vigente y es referente para la mayoría de las organizaciones

1.3.2. O-ISM3

O-ISM3 es una norma de madurez de la gestión de la seguridad de la información, publicado por The Open Group, define los define los procesos de seguridad para administrar un sistema de gestión de seguridad de la información (SGSI) en una organización, se debe definir los objetivos de seguridad requeridos en la Política de seguridad, ofrece un conjunto

de procesos de administración de seguridad a partir de los cuales la organización selecciona cuáles implementar en el SGSI (Canal, 2017).

En esta norma, cada proceso de control de seguridad en el SGSI devuelve métricas para indicar de qué manera este proceso está contribuyendo al logro de los objetivos de seguridad. Esta retroalimentación de las métricas diferencia a esta norma de otras que definen también un SGSI.

1.3.3. Serie ISO/IEC 27000

La serie de normas internacionales ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 emitidas por la Organización Internacional de Normalización (ISO) y la International Electronic (IEC) describe la manera en la que se debe gestionar la seguridad de la información en una organización, los conceptos relacionados con la seguridad y los sistemas de gestión, los requisitos de los SGSI, los controles de seguridad y la gestión de riesgos.

Por su parte Pallas (2009) estable que las normas de la serie ISO 27000, tienen como principales objetivos:

- Utiliza un marco metodológico que permita implementar un SGSI
- Indicar los controles para mitigar los riesgos.
- Gestionar los riesgos.
- Documentar las políticas, procedimientos, controles y metodología de tratamiento de riesgos.
- Asignar responsabilidades.
- Realizar un seguimiento y mejora continua.

Estas normas pueden ser implementada en organizaciones de cualquier tipo, pequeñas o grandes y de cualquier naturaleza, comerciales, educativas, de gobierno, etc. y proporcionan una metodología para diseñar e implementar un SGSI (Gómez & Andrés, 2012). Un resumen de algunas de las normas que conforman la serie ISO/IEC 27000 se incluyen en la Tabla 1 con las características o aspectos que cubren:

Tabla 1. Normas ISO 27000

Norma	Características
ISO/IEC 27000	Presenta una perspectiva general y los conceptos que se manejan.
ISO/IEC 27001	Indica los requisitos para implementar un SGSI es una norma certificable.
ISO/IEC 27002	Guía de buenas prácticas, describen los objetivos de control de seguridad.
ISO/IEC 27003	Detalla consejos de implementación de un SGSI de acuerdo ISO/IEC 27001.
ISO/IEC 27004	Guía para determinar métricas para medir un SGSI.
ISO/IEC 27005	Guía para realizar la gestión del riesgo en un SGSI.

Fuente: Elaboración propia. Adaptado de ISO/IEC27000:2018

1.3.3.1. ISO/IEC 27000:2018

Este estándar tiene una versión actualizada en el año 2018 y ofrece un enfoque completo de las otras normas de la misma serie. Establece los conceptos y una introducción a los sistemas de gestión de la seguridad de la información (SGSI).

1.3.3.2. ISO/IEC 27001:2013

Denominada por la ISO como "Tecnologías de la información - Técnicas de Seguridad - Sistemas de Gestión Seguridad de la Información – Requisitos". La revisión más reciente de esta norma fue publicada en el 2013, es la norma principal de la serie ISO/IEC 27000, su objetivo es establecer los requisitos para el diseño y la implementación de un SGSI de una forma bastante general de tal manera que sea aplicable a cualquier organización (ISO, 2013).

Según Kosutic (2016), la norma tiene una estructura funcional basada principalmente en la evaluación y el tratamiento de riesgos a los que la información puede estar expuesta, y pretende preservar las 3 características de la seguridad, es decir, la confidencialidad, integridad y disponibilidad, esta estructura se puede observar en la Figura 4.

Figura 4. Estructura de la ISO/IEC 27001.
Fuente: (Kosutic, 27001 Academy, 2016)

ISO/IEC 27001 está compuesta por 10 secciones y un anexo, en la Tabla 2 se indica un resumen de las principales secciones de la norma.

Tabla 2. Estructura de la norma ISO/IEC 27001

SECCIÓN	DESCRIPCIÓN
Sección 0	Introducción: objetivo de la norma.
Sección 1	Alcance: Puede ser aplicada a todo tipo de organización.
Sección 2	Referencias normativas: hace referencia a la ISO/IEC 27000.
Sección 3	Términos y definiciones: define los términos más utilizados.
Sección 4	Contexto de la organización: determina la organización, partes interesadas, requisitos y alcance del SGSI.
Sección 5	Liderazgo: apoyo de directivos al SGSI, estableciendo roles y responsabilidades y aprobando la política de seguridad de la información.
Sección 6	Planificación: realizar la gestión de riesgos, llenar la declaración de aplicabilidad, plantear los objetivos de seguridad de la información.
Sección 7	Apoyo: contar recursos financieros, difusión y control de documentos.
Sección 8	Funcionamiento: implementación de la gestión de riesgos, y de los controles y procesos para cumplir con los objetivos de seguridad.
Sección 9	Evaluación del desempeño: monitoreo, medición, análisis, evaluación, auditoría interna del funcionamiento del SGSI.

SECCIÓN	DESCRIPCIÓN
Sección 10	Mejora: para una mejora continua identifica como realizar las medidas correctivas.
Anexo A	114 controles de seguridad, agrupados en 14 dominios de seguridad.

Fuente: Noma ISO/IEC 27001:2013

La norma ISO/IEC 27001 en estas secciones establece los requisitos para el desarrollo y operación del SGSI, incluyendo un conjunto de controles en el anexo A, que forman parte del diseño de un SGSI y se los utiliza para mitigar los riesgos de seguridad, la norma no exige que se cumplan todos los controles sino solamente los que sean aplicables a cada organización (Kosutic, 2016) .

1.3.3.3. ISO/IEC 27002:2017

Denominada por la ISO como "Tecnología de la información - Técnicas de seguridad - Código de práctica para controles de seguridad de la información". De acuerdo con Gómez & Fernández (2018), esta norma proporciona un código de buenas prácticas para la gestión de la seguridad de la información, siendo un apoyo en el uso de la norma ISO/IEC 27001.

Presenta un conjunto de 114 controles, agrupados en 14 dominios de seguridad, estos controles también están listados en el Anexo A de la norma ISO/IEC 27001, se la utiliza como referencia para seleccionar controles de seguridad en el diseño e implementación de un SGSI y proporciona una descripción sobre la implementación de dichos controles (ISO, 2017). En la práctica, la mayoría de las organizaciones que adoptan ISO / IEC 27001 también adoptan ISO / IEC 27002 (Valencia & Orozco, 2017). Los 14 dominios de seguridad que contempla la norma se muestran en la Tabla 3.

Tabla 3. Dominios de Seguridad

Ítem en la norma	Dominio
5	Políticas de Seguridad de la Información

Ítem en la norma	Dominio
6	Organización de la seguridad de la información
7	Seguridad de los recursos humanos
8	Gestión de activos
8	Control de acceso
10	Criptografía
11	Seguridad física y Ambiental
12	Seguridad de las Operaciones
13	Seguridad de las Comunicaciones
14	Adquisición, desarrollo y mantenimiento de Sistemas
15	Relaciones con Proveedores
16	Gestión de incidentes de seguridad de la Información
17	Gestión de Continuidad del Negocio
18	Cumplimiento

Fuente: Norma ISO/IEC 27002:2017

1.4. Metodología de la Gestión de Riesgos

Una de las actividades más importantes en el desarrollo de un SGSI es decidir la metodología de gestión de riesgos con la que se va a trabajar, ya que existen varias ya definidas que se pueden utilizar y que se alinean con la ISO/IEC 27001 (Vanegas & Pardo, 2014), o inclusive se puede adoptar una propia que cumpla con los requerimientos de la norma, sin embargo debe estar claramente establecida para poder repetirla, es decir que se pueda utilizar de la misma manera siempre, para que los resultados sean apropiados.

Las vulnerabilidades y amenazas que pueden presentarse frente a los activos de información determinan los riesgos de seguridad. La evaluación de estos debe identificar, cuantificar y priorizar los riesgos y definir criterios de aceptación de riesgos de acuerdo con los objetivos que la organización se plantee. Estos resultados deben orientar la elección de controles para proteger la información contra esos riesgos (ISO 27000, 2018).

La metodología de riesgo según Solarte y Rosero (2015) debe incluir:

- Comparar los riesgos estimados con los criterios de riesgo, de esta manera se puede determinar la importancia que presentan.
- Realizar de forma periódica, un análisis de riesgos para determinar si existen cambios en los requisitos de seguridad de la información y en la situación de riesgo.
- Las evaluaciones de riesgos deben ser sistemáticas, comparables y reproducibles.

La Figura 5 muestra un esquema de forma en la que trabaja la gestión de riesgos.

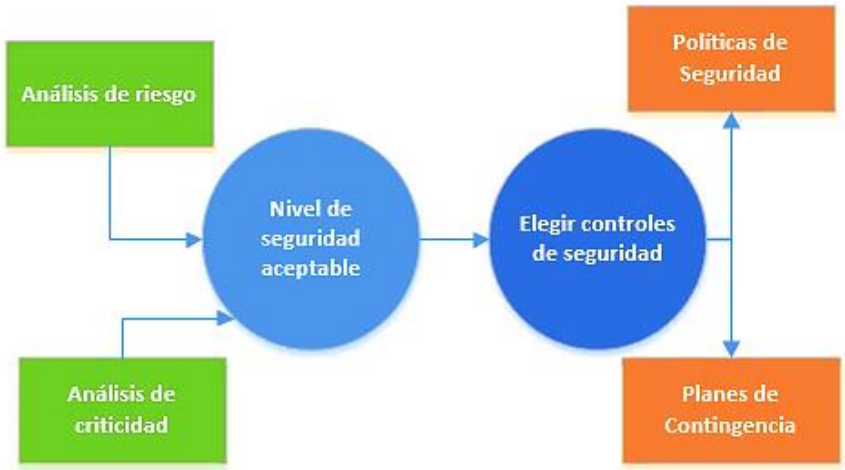


Figura 5. Esquema de la gestión de riesgos
Fuente: (Escrivá & Romero, 2013)

Los conceptos de vulnerabilidad, amenaza y riesgo están relacionados entre sí y son parte de la seguridad de la información, vulnerabilidades son las debilidades de seguridad de los sistemas de información, las amenazas son los posibles ataques internos o externos realizados aprovechando las vulnerabilidades y el riesgo es la manera en la que las amenazas se presentar (Escrivá & Romero, 2013).

Según Parra (2014), los conceptos asociados a la gestión de riesgos de acuerdo con la norma se listan a continuación:

Amenaza: la causa potencial de un incidente de seguridad que puede alterar el funcionamiento de una organización.

Riesgo: es la posibilidad de que una amenaza aproveche las vulnerabilidades de un activo de información.

Vulnerabilidad: debilidad de un activo u organización que puede aprovechar una amenaza.

Impacto: un cambio adverso en el funcionamiento de una organización.

En general las metodologías de gestión del riesgo tienen 2 etapas definidas: la evaluación del riesgo y el tratamiento del riesgo.

Evaluación del riesgo: Realiza una evaluación de las vulnerabilidades y las compara con el nivel de aceptación de riesgo definido. Los resultados de la evaluación de riesgos permiten realizar un informe de vulnerabilidades por cada criterio de seguridad de la información que determina la norma ISO/IEC 27002 (Alemán & Rodríguez, 2015).

Tratamiento del riesgo: Con los resultados de la evaluación del riesgo se deben establecer que acciones se realizarán para tratar los riesgos encontrados, esto se realiza normalmente seleccionando controles se seguridad, para conseguir un nivel de riesgo aceptable para la organización. Según la norma para el tratamiento del riesgo se tienen cuatro alternativas: reducir el riesgo, retener el riesgo, evitar el riesgo o transferir el riesgo (Alemán & Rodríguez, 2015).

Las metodologías más utilizadas para la gestión de riesgos son las siguientes:

1.4.1. MAGERIT

Utilizada por las empresas públicas españolas enfocado a la gestión de riesgos de la información. MAGERIT implementa la gestión de riesgos dentro de un marco de referencia que les permita a las organizaciones tomar decisiones a partir de los riesgos encontrados en el uso de las TI (MHAP, 2012).

Según Alemán & Rodríguez (2015) sus objetivos son: que la organización tome conciencia de la existencia de riesgos, ofrecer un método sistemático para analizarlo, ayudar en su tratamiento y prepararla para un proceso de certificación.

1.4.2. OCTAVE

Estándar desarrollado y publicado por el "Centro de Coordinación CERT" en *Carnegie Mellon University*. Constituye un método que permite evaluar el riesgo, para ello se basa en los conceptos de activos que incluye: individuos, hardware, software, datos y sistemas (Vanegas & Pardo, 2014).

Octave, es una metodología para empresas grandes; Octave-S, similar a la original, pero para empresas mediana; y Octave Allegro, una metodología con un proceso simplificado con un uso más fácil (García, 2015).

1.4.3. ISO 31010

Desarrollada por ISO/IEC para gestionar riesgos en sentido general. Para ello se basa en test y análisis que permiten tomar decisiones acerca de la selección y tratamiento de riesgos. Esta norma se basa en la políticas y procedimientos que contienen todos los niveles de una entidad (Vanegas & Pardo, 2014).

1.4.4. RISK IT

Publicado por ISACA, es un marco de referencia que se enfoca en las TIC, proporciona una visión global de los riesgos de la organización, es una herramienta práctica para la gestión de riesgos basada en el valor y beneficios que la organización obtiene a través de sus proyectos tecnológicos, se concentra en el cumplimiento de los objetivos de la organización. Este modelo puede utilizarse en cualquier tipo de empresa, y ofrece una serie de guías para la gestión eficaz de los riesgos (Vanegas & Pardo, 2014).

1.1.1. ISO/IEC 27005

Denominada "Tecnología de la Información - Técnicas de Seguridad - Gestión de riesgos de la Seguridad de la Información". Su objetivo es proporciona directrices para gestionar los riesgos de seguridad de la información en una organización, no proporciona una metodología específica para la gestión de riesgos, sino que cada organización debe definir un enfoque propio para dicha gestión, dependiendo del alcance del SGSI, los objetivos de seguridad o el análisis de las metodologías existentes (ISO 27005, 2018).

Es compatible con los requerimientos que establece la norma ISO/IEC 27001 en la sección 6. En la Figura 6 se indica los pasos establecidos para la gestionar los riesgos.

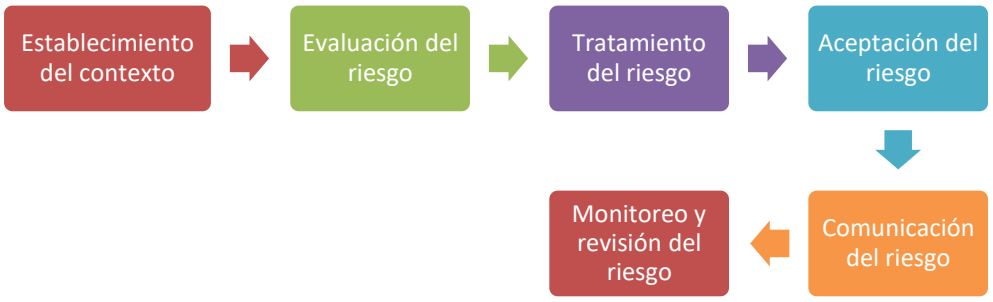


Figura 6. Ciclo de la gestión de riesgos
Fuente: (ISO 27005, 2018)

El estándar no especifica, ni recomienda ningún método para la gestión de riesgos. Da una serie de buenas prácticas para gestionarlo, además de ejemplos de cómo realizar esta gestión. La Tabla 4 presenta la distribución de las actividades de la gestión del riesgo en la seguridad de la información en las fases del ciclo de mejora continua (ISO 27005, 2018):

Tabla 4. Pasos de la Gestión de Riesgo

Etapas	Gestión del riesgo
Planificar	Establecer el contexto Valoración del riesgo Planificación del tratamiento del riesgo Aceptación del riesgo
Hacer	Implementación del plan de tratamiento del riesgo
Verifica	Monitoreo y revisión continuos de los riesgos
Actuar	Mantener y mejorar el proceso de gestión del riesgo en la seguridad de la información

Fuente: (ISO 27005, 2018)

La norma ISO/IES 27005 establece que los activos de información pueden ser de 2 tipos: activos de procesos y activos de soporte, los segundos dan soporte a los primeros y permiten que estos funcionen de manera adecuada, en la Tabla 5, se presenta la clasificación de los activos, los elementos que la componen y sus características:

Tabla 5. Tipos de activos de información

TIPO DE ACTIVO	ELEMENTOS	CARACTERÍSTICAS
Activos primarios	Actividades y	Procesos cuya pérdida o degradación

TIPO DE ACTIVO	ELEMENTOS	CARACTERÍSTICAS
	procesos del negocio	pueden impedir cumplir la misión u objetivos de la organización
	Información	Información estratégica para la organización, personal privada, etc.
Activos de soporte (dependen los activos primarios)	Hardware	Equipos que dan soporte a los procesos, computadores, servidores, etc.
	Software	Programas o aplicaciones necesarios para el funcionamiento de los procesos.
	Redes	Dispositivos de telecomunicaciones
	Personal	Personas involucradas con los sistemas de información.
	Sitio	Lugares, medios físicos o servicios que se requieren (Internet, energía eléctrica, etc.)
	Estructura de la organización	Estructura organizacional

Fuente: (ISO 27005, 2018)

CAPÍTULO II: MARCO METODOLÓGICO

2.1. Enfoque metodológico de la investigación.

En este capítulo se indica el marco metodológico utilizado, tipo y diseño de investigación, la población, muestra, los instrumentos de recolección de datos y las técnicas para el procesamiento de estos datos.

En el presente trabajo de investigación se ha realizado una investigación de tipo descriptiva, que según Hernández Sampieri & Fernández (2012), "*los estudios descriptivos permiten especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis*", ya que se ha realizado una descripción de la situación actual de la Universidad, se realizó un inventario de los activos de información, identificó los riesgos y determinó el tratamiento adecuado de estos, según los objetivos establecidos inicialmente, la presente investigación será abordada desde un enfoque cuantitativo, ya que se va a medir, comparar y describir las variables .

2.2. Población, unidades de estudio y muestra.

2.2.1. Población

Para Hernández Sampieri & Fernández (2012), "*la población o universo es un conjunto de todos los casos que concuerdan con determinadas especificaciones*", para este proyecto de investigación comprende la comunidad universitaria que está distribuida en tipos de población como se muestra en la Tabla 6:

Tabla 6. Distribución de población

UNIDAD ADMINISTRATIVA	PERSONAL
Directivos	17
Docentes	12
Administrativos	15
TOTAL	44

Fuente: elaboración propia

2.2.2. Muestra

Siendo la muestra según Hernández Sampieri & Fernández (2012), "*un subgrupo de la población de interés sobre el cual se recolectarán datos, y que tiene que definirse y delimitarse de antemano con precisión, además de que debe ser representativo de la población*", para el presente proyecto de investigación, en un consenso con las autoridades de la Institución se tomará en cuenta como una fase inicial el personal de la Dirección Académica, la Dirección Financiera, Talento Humano y la Dirección de Tecnología de la Información y Comunicación (TIC), que son las áreas que manejan los sistemas de información estratégicos de la organización.

La muestra en este caso es un muestreo intencional o de conveniencia, ya que se tomará el grupo de personas que corresponden a los responsables del manejo de activos de información en cada una de las direcciones y fue de 27 personas, distribuidos de la manera que se indica en la Tabla 7.

Tabla 7. Distribución de personal en las Direcciones

UNIDAD ADMINISTRATIVA	PERSONAL	
Dirección Académica	Directivos	7
	Docentes	12
	Administrativos	3
Dirección Financiera	Directivos	1
	Administrativos	2
Dirección de Talento Humano	Directivos	1
Dirección TIC	Directivos	1
TOTAL		27

Fuente: elaboración propia

2.3.Técnica de recolección de datos

Como técnicas de recolección de datos se utilizaron: encuestas, entrevistas, fichas de observación y evidencia documental.

2.3.1. Encuestas

Según González, Gallardo, & Pozo (2017), "*La encuesta es una técnica que recoge información a grupos de personas sobre los hechos o fenómenos que se investigan (…) y son recomendados cuando lo que interesa es conocer la situación general y no casos particulares*".

Se realizó una encuesta (ver Anexo 1) que se aplicó a la muestra seleccionada para determinar la cultura institucional sobre seguridad de la información, es decir el conocimiento que tienen sobre esta y la existencia de políticas, normas y procedimientos de seguridad de la información.

Los datos obtenidos se tabularon y valoraron, mostrándose los resultados obtenidos en cada cuestionario en el numeral 2.6 Situación actual.

2.3.2. Entrevistas

La entrevista estructurada de acuerdo con González, Gallardo, & Pozo (2017), "*es aquella que de acuerdo con el objetivo previsto se ha preparado las preguntas con anterioridad*". Se realizó entrevistas a personal de las direcciones Académica, Financiera, Talento Humano y TIC (Anexo 2), y se utilizó para realizar el inventario inicial de activos de información que consideran importante para sus funciones, para la valoración de dichos activos con un nivel de criticidad en el caso de que ocurra un evento de seguridad que afecte la disponibilidad, integridad o confidencialidad y el análisis de las amenazas y vulnerabilidades que pueden presentarse para cada activo.

2.3.3. Observación directa

Para realizar la evaluación de riesgos, se utilizó la observación directa con una lista de chequeo donde se estableció los activos más importantes desde el punto de vista de los procesos de negocio, en el que se describe también el nivel de criticidad de cada activo, tomando como punto de partida las entrevistas realizadas a las personas responsables de los procesos.

2.4. Formas de procesamiento de la información

Para el procesamiento de la información obtenida mediante los instrumentos se utilizó la estadística descriptiva para presentar los resultados obtenidos, se tabularon los resultados y se presentan los gráficos resultantes. Esta información se muestra en el acápite 2.5. Situación Actual, lo cual permitió conocer el estado inicial de la seguridad de la información en la UNIBE.

2.5. Situación Actual

Parte de la situación actual fue conocer cuán extendida está la cultura de seguridad de la información en la Universidad, lo que se consiguió con una encuesta realizada a todos los empleados de la institución, tanto directivos, como docentes y administrativos. Los resultados de la encuesta son los siguientes:

En respuesta a la pregunta ¿Sabe o ha escuchado usted qué es la Seguridad de la Información? Los resultados se muestran en la Figura 7.

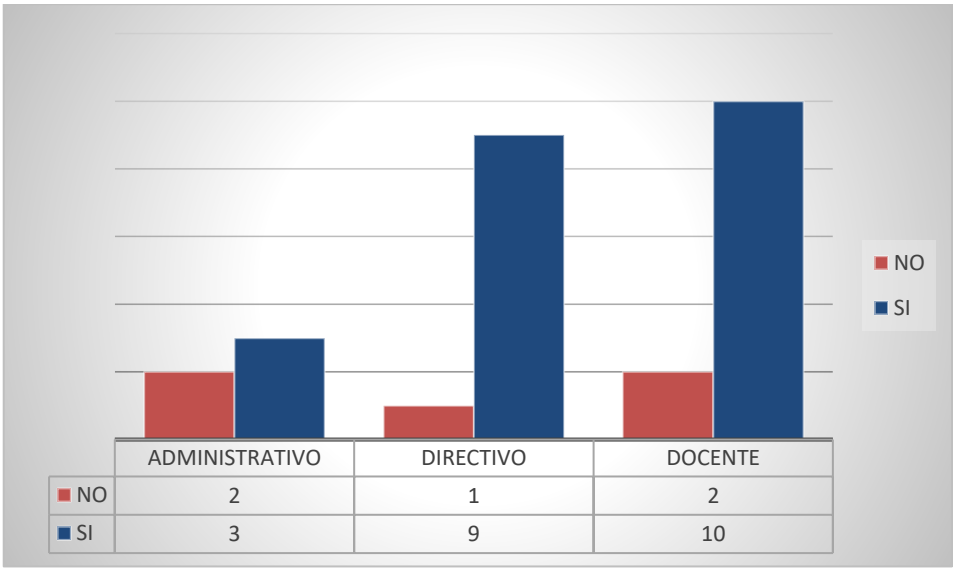


Figura 7. Seguridad de la Información
Fuente: Elaboración propia

Cómo puede observarse de los resultados mostrados, el 80% de los administrativos, es decir 12 personas, el 94,1% de los directivos, 16 personas y el 83,3% de los docentes encuestados que sería 10 personas ha escuchado o sabe a qué se refiere la seguridad de la información, en cambio el 20% de los administrativos (3 personas), el 5,9% de los directivos (1 persona) y el 16,7 % de los docentes (2 personas) no sabe a qué se refiere la seguridad de la información. En general los directivos y los administrativos que manejan los sistemas de información de la Universidad tienen un mayor entendimiento de las consecuencias que la pérdida de seguridad de la información tendría en su trabajo cotidiano.

Si se toma en cuenta en cambio el total de los encuestados se puede deducir que el 81% de todos los empleados encuestados, es decir 22 personas conoce o ha escuchado sobre la seguridad de la información, mientras que el 19% es decir 5 personas no conoce o no sabe sobre este concepto, estos resultados se muestran en la Figura 8.

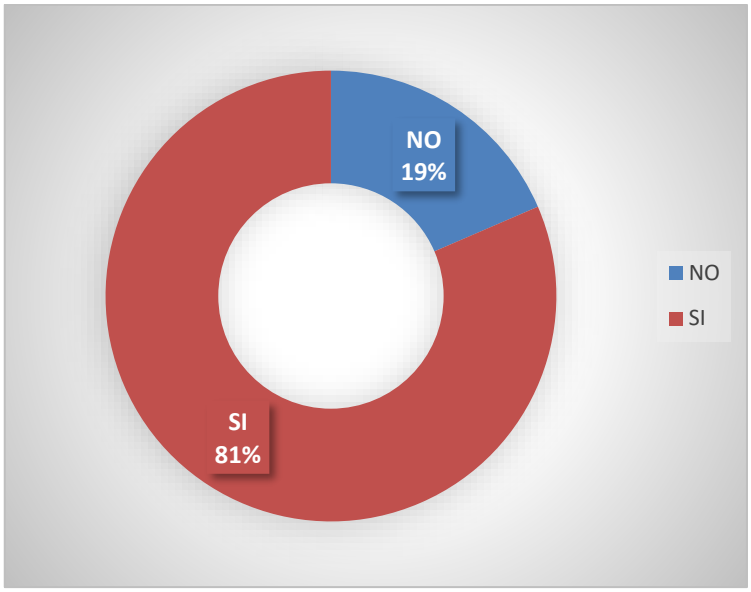


Figura 8. Porcentajes totales
Fuente: Elaboración propia

Esto demuestra una fortaleza de la Universidad considerando que la implementación y la difusión del SGSI puede resultar más fácil de entender para los miembros de la institución, puesto que de acuerdo con la norma una de las tareas a realizar es la concienciación y formación de toda la organización.

En respuesta a la pregunta ¿Conoce Usted si la UNIBE cuenta con una política de Seguridad de la Información? Los resultados se muestran en la Figura 9, y permite determinar que entre los administrativos un 80% de encuestado cree que la Universidad no cuenta con una política de seguridad de la información y un 20% cree que si existe la política. Entre los directivos en cambio el 100% piensa que no existe o no han escuchado de ésta. Y por último entre los docentes un 83,3% creen que no existe política de seguridad y un 16,7% piensa que existe. De acuerdo con la revisión en sitio se ha podido determinar que la política de seguridad de la información no se ha generado anteriormente en la institución.

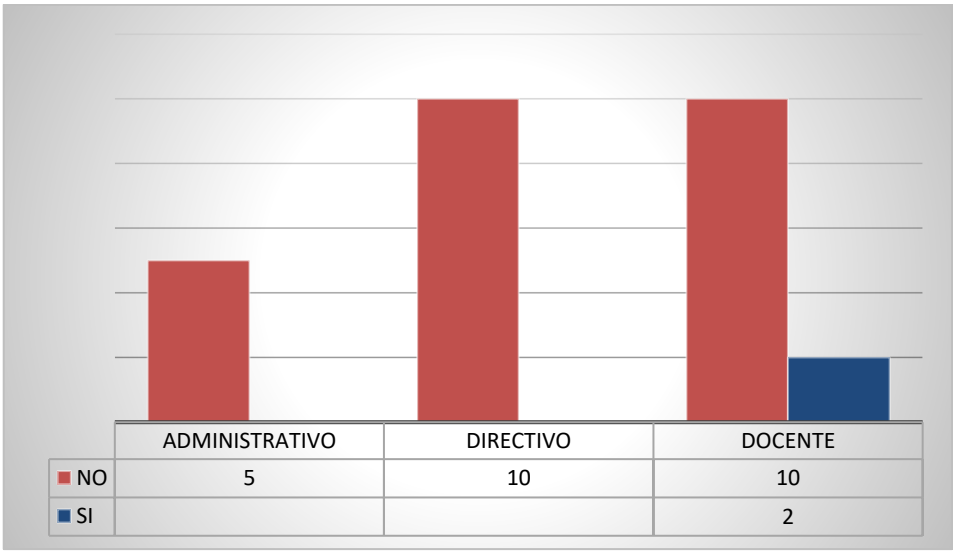


Figura 9. Política de Seguridad de la información
Fuente: Elaboración propia

En cuanto a la pregunta ¿Ha recibido capacitación acerca de la importancia de la seguridad de la Información dentro de la UNIBE? Se puede ver los resultados en la Figura 10 en la que el 100% de los administrativos, el 100% de los directivos y el 100% de los docentes encuestados contestó negativamente esta pregunta. En general se puede observar que en la institución hasta el momento no se ha tratado el tema de la seguridad de la información y cómo no hay políticas definidas, tampoco se ha capacitado sobre los procedimientos y normas de seguridad a aplicar.

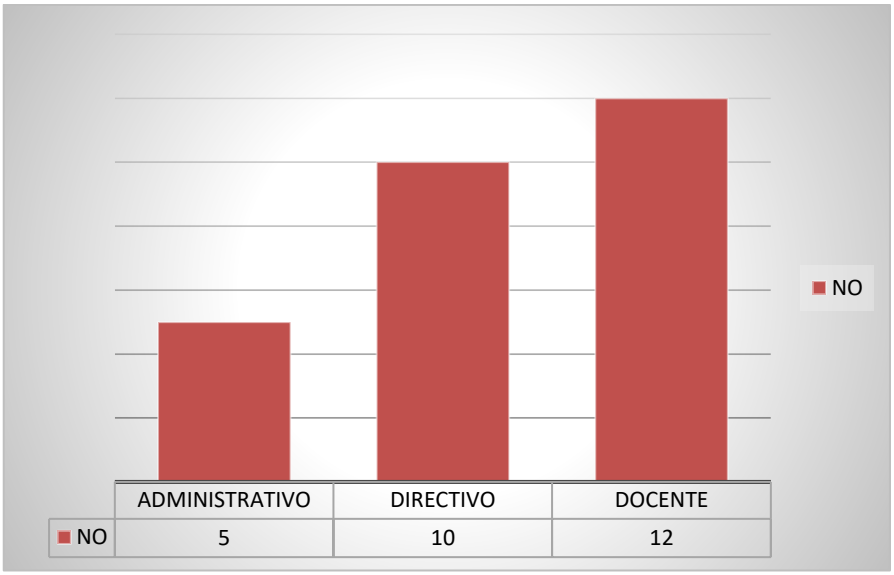
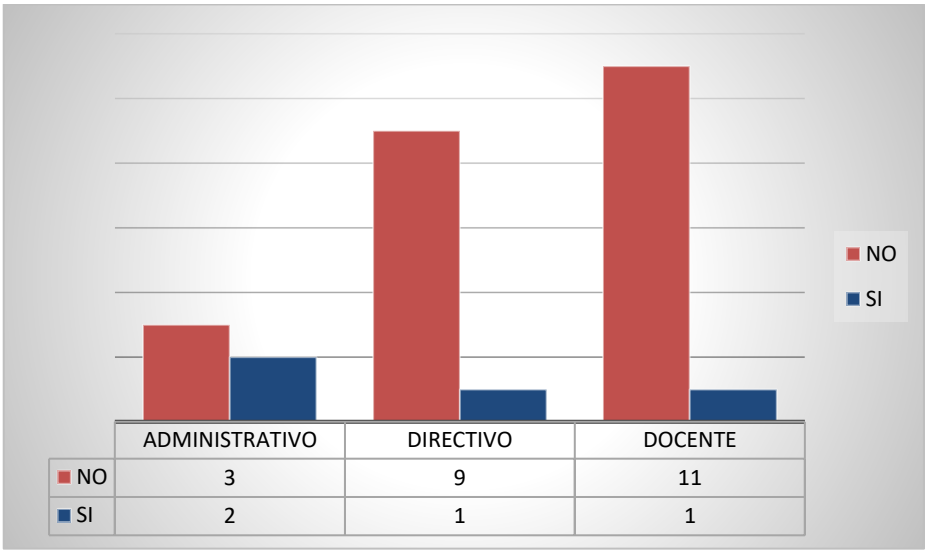


Figura 10. Capacitación sobre Seguridad de la Información
Fuente: Elaboración propia

Para la pregunta ¿Si se produjera un incidente de seguridad de la información, sabe cómo

proceder? (pérdida de información, documentos, equipos, etc.) se obtuvo los resultados indicados en la Figura 11, el 95.18% de todos los encuestados no sabría qué hacer en caso de producirse un incidente que afecte la seguridad de equipos o documentos a su cargo. Esto se determina como una debilidad de la institución y es consecuencia de la falta de capacitación sobre la seguridad de la información y la falta de procedimientos sobre la comunicación y el tratamiento de incidentes de seguridad que involucre tanto a equipos como a documentos



	ADMINISTRATIVO	DIRECTIVO	DOCENTE
NO	3	9	11
SI	2	1	1

Figura 11. Sabe qué hacer en un incidente de seguridad

Fuente: elaboración propia

Por lo que puede observarse de las respuestas de la pregunta ¿Piensa usted que es importante generar dentro de la comunidad universitaria una cultura sobre Seguridad de la Información? que se indican en la Figura 12, el 100% de encuestados consideran importante generar una cultura de seguridad de la información y están de acuerdo en que la información debe protegerse, porque es importante para la organización y para las funciones que desempeñan. Esta sería una fortaleza de la Universidad debido a esta percepción que tiene de la importancia de la seguridad de la información puede ayudar a crear un clima propicio para la implementación de un SGSI en la institución.

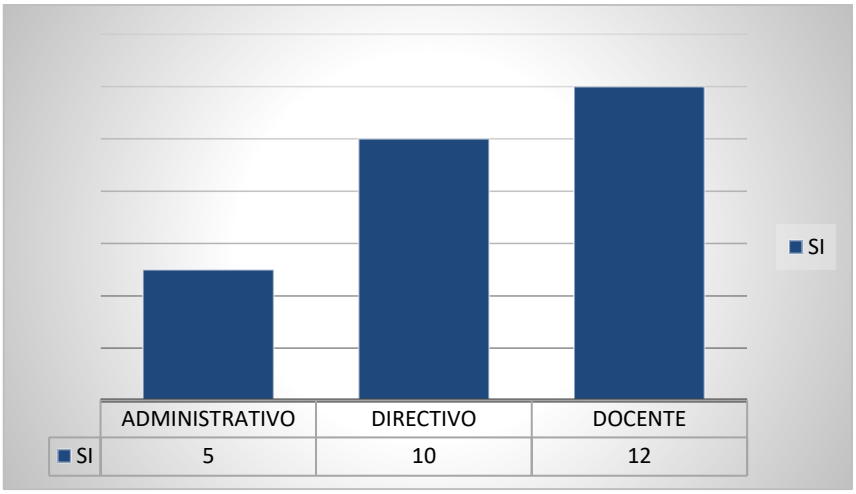


Figura 12. Generar cultura de Seguridad de la Información
Fuente: elaboración propia

Para la pregunta ¿Tiene usted identificada la información que utiliza en sus actividades? Los resultados se muestran en la Figura 13, en la que se puede observar que el 100% de los entrevistados tiene identificada la información que utiliza en sus actividades o procesos, por lo que se puede realizar con mayor facilidad un inventario de los activos de información que están bajo su responsabilidad, los entrevistados son personas que manejan los sistemas de información de la Universidad.

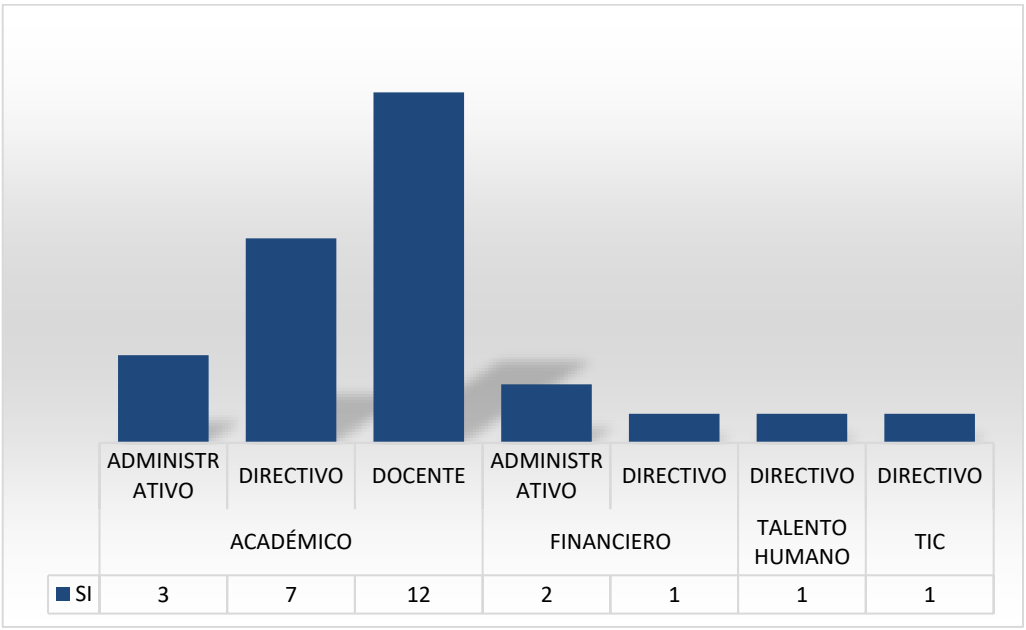


Figura 13 Identificada información que utiliza
Fuente: Elaboración propia

En respuesta a la pregunta ¿Los procesos en su dirección y/o unidad están claramente definidos? se observa en la Figura 14 que el 81% de los encuestados, es decir 22 personas piensa que si están definidos los procesos en el área en la que trabaja, mientras que el 19% es decir 5 personas no sabe o cree que los procesos no están claramente definidos. Sin embargo, después de la entrevista se pudo determinar que la Universidad está trabajando en un proceso de Gestión de Calidad en el que se están definiendo todos los procesos de la institución, los procesos en las áreas de estudio están ya definidas, pero falta la socialización a todo el personal.

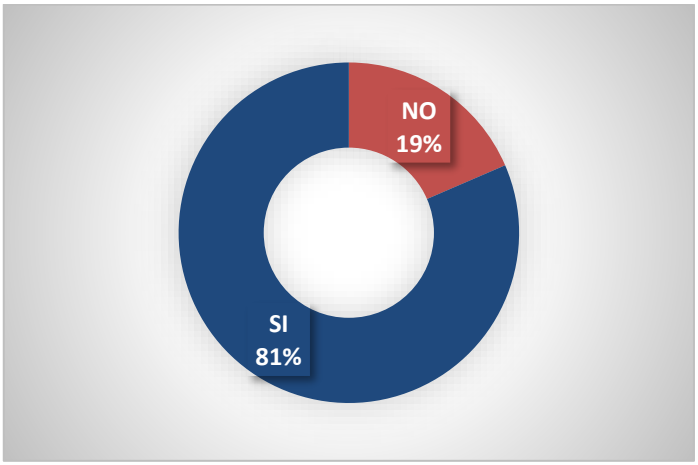


Figura 14 ¿Procesos definidos claramente?
Fuente: Elaboración propia

Para la pregunta ¿Sabe cuál es el tiempo de retención de la información de la que usted es responsable? se observa en la Figura 15 que, en los procesos Financiero, Talento Humano y TIC, el 100% de los encuestados conoce el tiempo de retención de la información que maneja, en cambio en el proceso Académico, el 81,1% de los encuestados no conoce el tiempo de retención de la información que maneja, frente al 18,2% que respondieron afirmativamente.

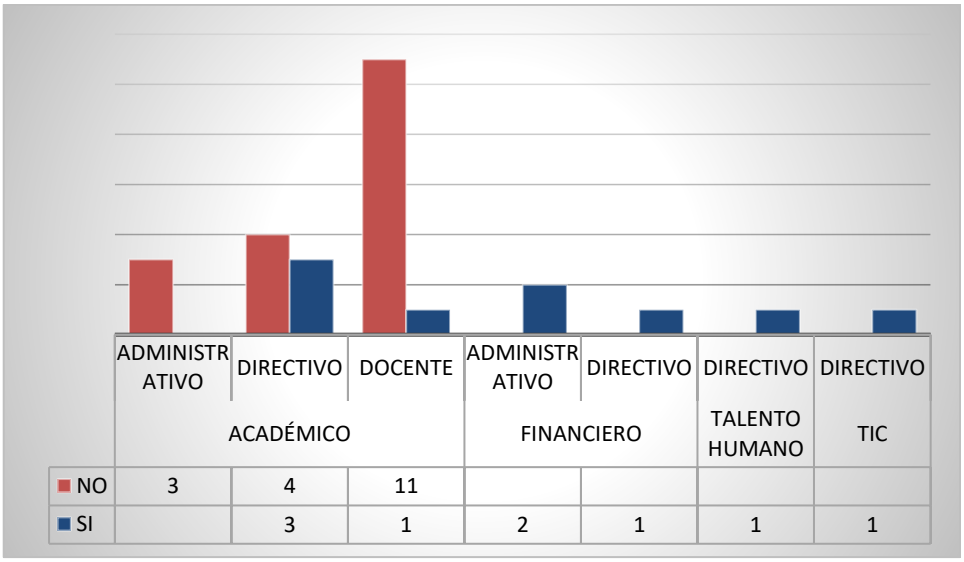


Figura 15 Tiempo de retención de la información
Fuente: Elaboración propia

Para la pregunta ¿Sabe usted el procedimiento que hay que seguir para destruir información? en las respuestas indicadas en la Figura 16 se puede concluir que el 100% de los encuestados desconoce el procedimiento a seguir para destruir información interna o confidencial, los resultados evidencian una debilidad clara en el manejo de la información.

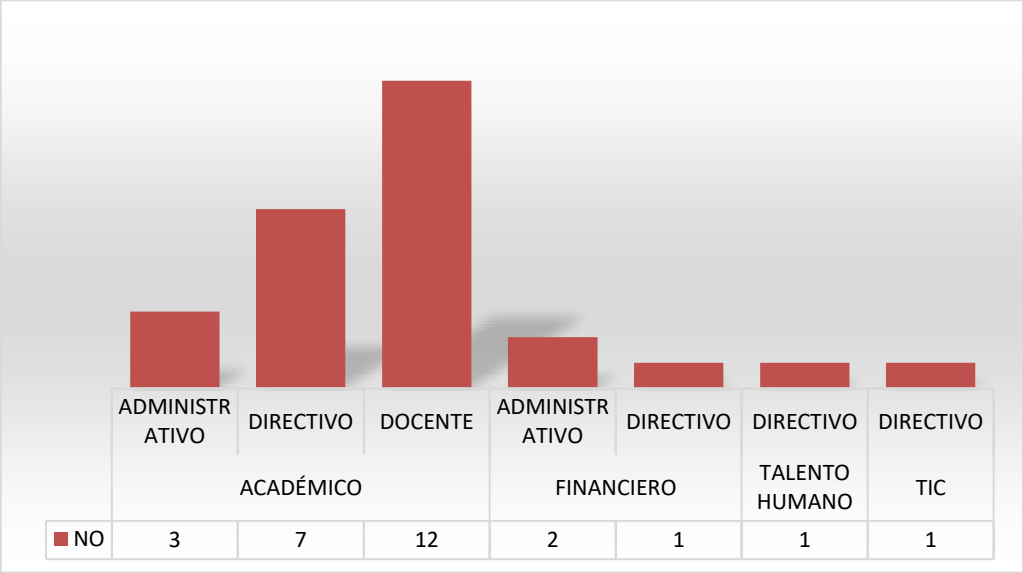


Figura 16 Procedimiento para destruir información
Fuente: elaboración propia

De aquí se puede ver que la Institución no posee en la actualidad con un sistema de gestión de la seguridad de la información (SGSI), ni con una política de Seguridad de la Información, los procedimientos de seguridad existentes son los que cada persona considera apropiadas para su trabajo; por tanto, es importante desarrollar el SGSI y un Plan Director de Seguridad

con el objetivo de mejorar la seguridad de la información en toda la institución, adaptándola a la norma ISO/IEC 27001.

Tampoco ha existido capacitación sobre la seguridad de la información ni sobre procedimientos, reglamentos o normas al respecto o cómo proceder en caso de que exista un incidente de seguridad que involucre activos de información.

Se ha logrado determinar las fortalezas y debilidades que pueden influir en la implantación de un Sistema de Seguridad de la Información y la situación inicial de la cultura de seguridad de la información en los empleados de la UNIB.E.

Adicionalmente mediante la entrevista se pudo determinar un inventario preliminar de activos de información con detalles del medio en el que se encuentran (físico o digital), el tipo de información (interna, confidencial, externa) y el impacto de que se presente una amenaza sobre su disponibilidad, integridad y confidencialidad sobre dicha información.

2.5.1. Estado de madurez respecto a la norma ISO/IEC27001

Mediante las entrevistas realizadas a los responsables de los procesos y la observación directa se ha levantado el nivel de madurez o estado inicial de la institución con respecto a los controles de los 14 dominios de seguridad del SGSI establecidos en el Anexo A de la norma ISO/IEC 27001, el resultado se puede observar en la Tabla 8, en la que se ha determinado el porcentaje de cumplimiento de dichos controles.

Tabla 8. Estado de madurez SGSI

Evaluación estado de madurez SGSI	SI	NO	Cumplimento
A.5 Políticas de seguridad de la información			**0%**
¿Existe documentos de política de seguridad?		x	0%
¿Existe normas y procedimientos sobre la seguridad de la información?		x	0%
A.6 Organización de la seguridad de la información			**17%**
¿Existen roles y responsables definidos en cuanto a la seguridad de la información?		x	0%
¿Existen política y controles de seguridad sobre usuarios móviles?		x	0%
¿Se mantienen y controlan los equipos portátiles para garantizar que estén actualizados y libres de virus?	x		50%

Evaluación estado de madurez SGSI	SI	NO	Cumplimento
A.7 Seguridad de los recursos humanos			**40%**
¿Se realiza una verificación de referencias y antecedentes durante el proceso de selección de personal?	x		100%
¿Están definidos los términos confidencialidad y responsabilidad en los contratos?	x		80%
¿Existe un programa de concientización / educación sobre la seguridad de la información para todos los empleados?		x	0%
¿Existe un proceso disciplinario para incidentes de seguridad de la información, provocados por los empleados? (fraude, hackeo, etc.)		x	0%
¿Existe procedimientos para recuperación de activos de información, eliminación de los derechos de acceso, cuando el empleado acaba su relación laboral?	x		20%
A.8 Gestión de los activos			**18%**
¿Existe un inventario de activos de información?		x	0%
¿Los activos tienen propietario de riesgo?		x	0%
¿Existe procedimientos para clasificación y etiquetado de la información?	x		50%
¿Existe una política sobre el uso de correo electrónico, Internet?		x	0%
¿Hay controles apropiados para mantener la confidencialidad de los datos almacenados?	x		40%
A.9 Control de acceso			**35%**
¿Existe normas para el control de acceso y perfiles de usuario?	x		20%
¿Se utiliza autenticación para acceso a redes, sistemas y aplicaciones críticas?	x		60%
¿Se genera solicitud de creación de usuarios y se registra apropiadamente?		x	0%
¿Se revisa y se retira id de usuario en desuso?	x		60%
A.10 Criptografía			**0%**
¿Existe controles criptográficos?		x	0%
A.11 Seguridad física y del entorno			**51%**
¿Se utilizan sistemas de control de acceso a las instalaciones, ingreso CCTV, etc.?	x		70%
¿Existe un control de acceso autorizado a las áreas críticas?	x		60%
¿Existe protección contra catástrofes naturales, incendio, etc.?	x		60%
¿TIC y el equipo relacionado se encuentran en áreas protegidas?	x		50%

Evaluación estado de madurez SGSI	SI	NO	Cumplimento
¿Existe protección contra fallas de energía eléctrica?	x		60%
¿Se realiza mantenimientos periódicos de los equipos de cómputo, red y telecomunicaciones?	x		50%
¿Se realiza una eliminación adecuada de la información de los equipos que se dan de baja?	x		60%
¿Existe la cultura de no dejar los equipos con claves ingresadas y los escritorios sin documentación importante?		x	0%
A.12 Seguridad de las operaciones			**67%**
¿Existen procedimientos para las operaciones de TI, sistemas y gestión de redes, gestión de incidencias, la administración de TI, seguridad de TI, seguridad física, gestión de cambios, etc.?	x		60%
¿Existen controles de detección, prevención y recuperación contra programas maliciosos?	x		70%
¿Existen políticas y procedimientos para la realización de copias de seguridad?	x		70%
A.13 Seguridad de las comunicaciones			**65%**
¿Existen procedimientos para la administración de las operaciones de sistemas e infraestructuras de red?	x		60%
¿Existe una segmentación de red adecuada usando cortafuegos, VLAN, VPN, etc.?	x		70%
A.14 Adquisición, desarrollo y mantenimiento de sistemas			**0%**
¿Existen requisitos de seguridad para la adquisición de aplicaciones y software?		x	0%
A.15 Relaciones con los proveedores			**0%**
¿Existen procedimientos para las relaciones con proveedores que involucran servicios de TI?		x	0%
A.16 Gestión de incidentes de seguridad de la información			**0%**
¿Existen procedimientos para notificación, evaluación y respuesta a incidentes de seguridad?		x	0%
A.17 Gestión de continuidad del negocio			**0%**
¿Existe un plan de continuidad del negocio y análisis de impactos?		x	0%
¿Se tienen controles para recuperación de operaciones, capacidad de rendimiento, balanceo de carga?		x	0%
A.18 Cumplimiento			**10%**
¿Existen políticas y procedimientos para la adquisición y el uso de licencias de aplicaciones y software?		x	0%
¿Se capacita al personal en el manejo de información de carácter personal?	x		20%

Evaluación estado de madurez SGSI	SI	NO	Cumplimento
TOTAL			**22%**

Fuente: Elaboración propia en base a la norma ISO/IEC 27001

La Figura 17 muestra un gráfico radial del cumplimiento en las 14 categorías de control de la norma para la situación actual. Como se puede observar la institución está en un 22% de cumplimiento de los controles de un SGSI en el estado inicial del diseño, esto se debe a anteriormente no se ha implementado antes ningún Sistema de Gestión de Seguridad de la Información y no existen políticas ni normas formalmente definidos para la mayoría de los controles, hay sin embargo como producto de la implementación del Sistema de Calidad que la institución está llevando a cabo algunos procedimientos definidos para los procesos analizados.

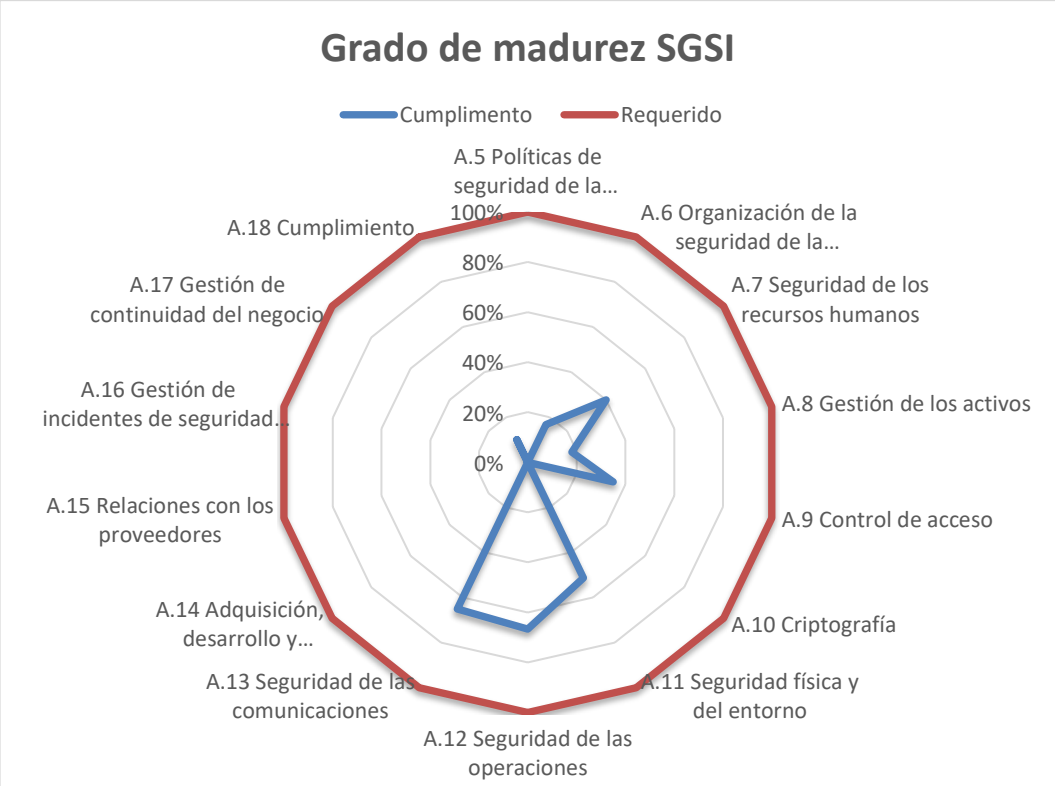


Figura 17. Grado de madurez respecto al SGSI
Fuente: elaboración propia

2.6. Metodología seleccionada

Para realizar el diseño del Sistema de Gestión de Seguridad de la Información SGSI se ha tomado en cuenta los pasos que establece la norma ISO/IEC 27001 y que se indican en la Figura 18 con las actividades que cada paso requiere. Como el objetivo del presente trabajo

de investigación es realizar el diseño del SGSI para la UNIB.E, las actividades a realizar están dentro del paso Planear del círculo de calidad de Deming, estas son: contexto de la organización, liderazgo y planeación.

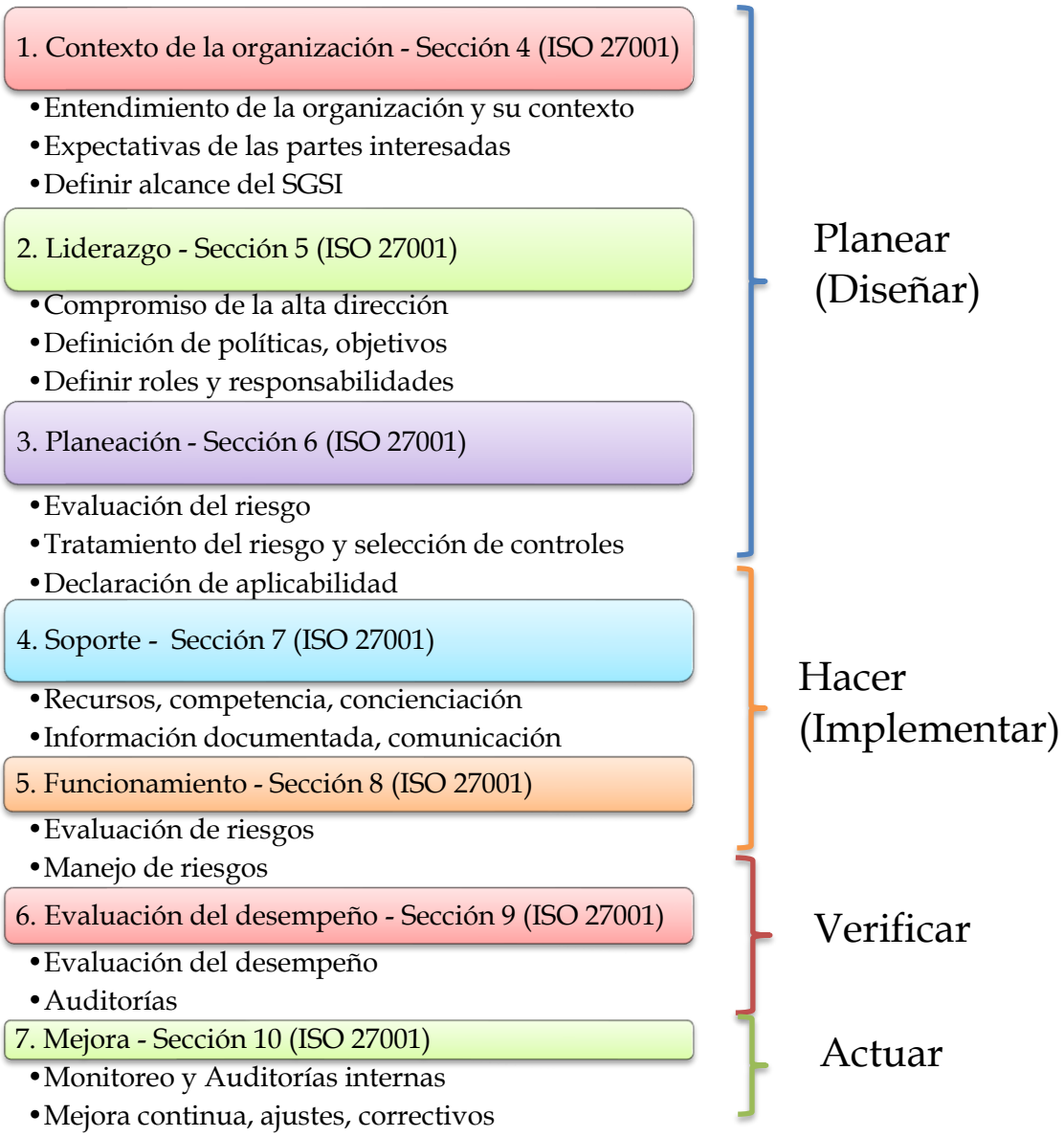


Figura 18. Pasos del SGSI de acuerdo con el ciclo de calidad y la ISO/IEC 27001
Fuente: (ISO, 2013)

El diagrama de bloques de la metodología utilizada para el diseño del SGSI en el ciclo Planear indicado puede observarse en la Figura 19.

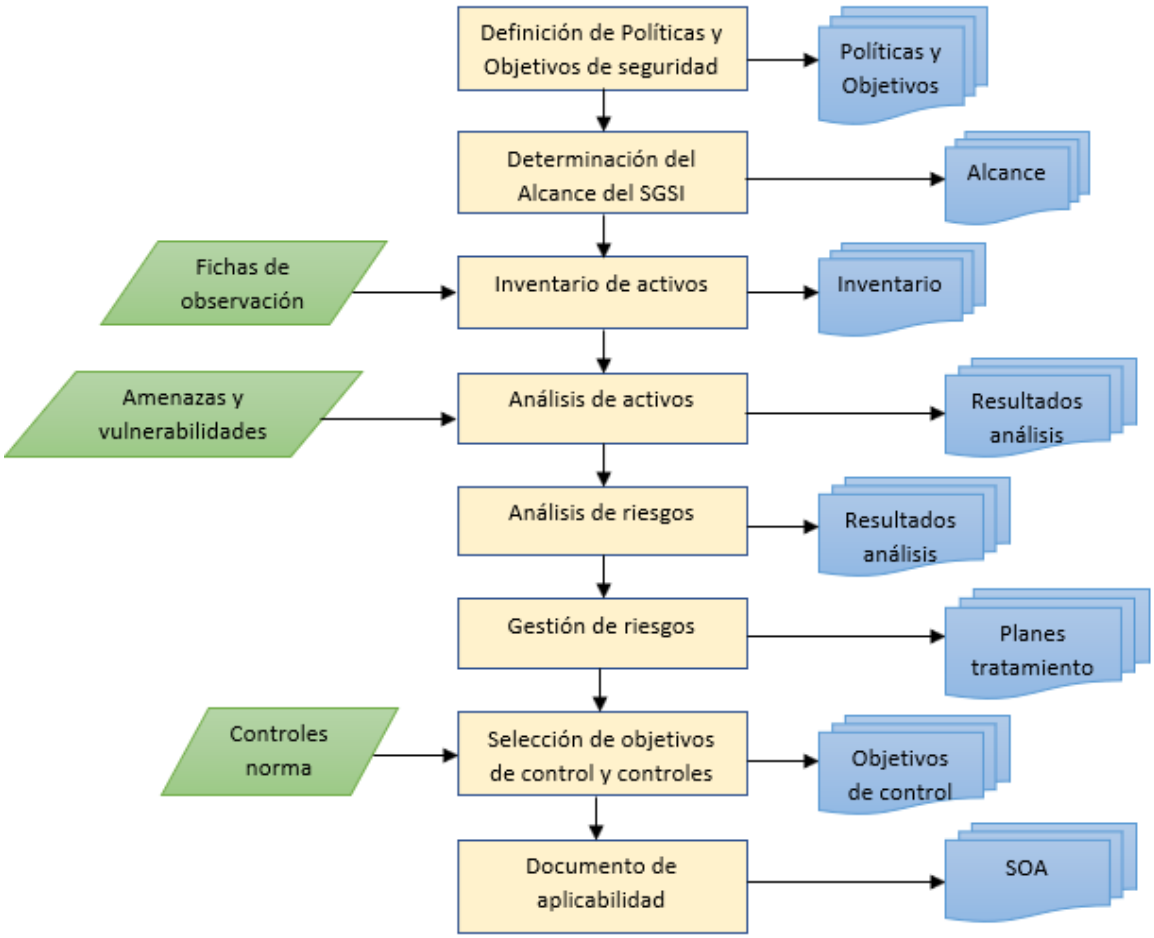


Figura 19. Diagrama de Bloques de la Metodología
Fuente: (ISO, 2013)

Con las actividades que define la norma ISO/IEC 27001 y el diagrama de bloques de la Figura 19, la metodología para el diseño del SGSI constará de 4 fases cada una con diferentes actividades como se resume en la Tabla 9.

Tabla 9. Fases del diseño de SGSI

FASES	ACTIVIDADES	DESCRIPCIÓN
Fase 1: Contexto de la organización	Situación actual	Encuesta a los empleados de la institución, observación en sitio.
	Estructura de la institución	Documentación de la institución
Fase 2: Liderazgo	Definir el alcance del SGSI	Entrevista directivos de la Institución y Directores de las áreas.
	Objetivos del SGSI	Entrevista directivos de la Institución y Directores de las áreas.
	Desarrollar la política de seguridad para la Institución.	Entrevista directivos de la Institución y Directores de las áreas.
	Definir roles y responsabilidades	Entrevista directivos de la Institución y Directores de las áreas.
Fase 3: Planeación: Gestión de riesgos de la información	Inventario de activos de información	Entrevista a los responsables de las áreas y personal que maneja los sistemas de información.
	Determinar metodología de gestión de riesgos	Descripción de la metodología a utilizar.
	Valoración de riesgos	Ficha de observación para identificación de riesgo a los activos.
	Determinar el tratamiento de los riesgos	Definición de tratamiento.
	Elegir los objetivos de control y los controles de seguridad para los riesgos determinados	Declaración de aplicabilidad
Fase 4: Diseño	Planes de tratamiento de riesgos	Definición de proyectos
	Plan de implementación SGSI	Definición del plan de implementación

Fuente: Elaboración propia

CAPÍTULO III: PROPUESTA

3.1. Fundamentos de la propuesta

Para el desarrollo del presente trabajo se seguirán los pasos que determina la norma ISO/IEC27001 para el desarrollo de un SGSI, adicionalmente se elegirán los controles de seguridad que la ISO/IEC27002 establece y que sean adecuados para la Universidad, de acuerdo con el resultado que se determine de la gestión de riesgos. De acuerdo con el apartado 2.6 metodología seleccionada se definió las fases de la propuesta que son:

- Fase 1: Contexto de la organización
- Fase 2: Liderazgo
- Fase 3: Planeación: Gestión de riesgos de la información
- Fase 4: Plan de Implementación del SGSI

Durante el proyecto de implementación del SGSI se deben redactar los siguientes documentos:

- **Alcance del Sistema de Gestión de Seguridad de la Información**: se refiere a los procesos o áreas que forman parte del SGSI.
- **Política de seguridad de la información**: políticas de alto nivel que van a regular la seguridad de la información en la institución.
- **Inventario de activos**: los activos dentro del alcance del SGSI, incluyendo la determinación de los propietarios de los activos.
- **Metodología de evaluación y tratamiento de riesgos**: descripción de la metodología para gestionar los riesgos de la información.
- **Declaración de aplicabilidad**: determina los objetivos y la aplicabilidad de cada control establecido en el Anexo A de la norma ISO 27001.
- **Planes de tratamiento de riesgos**: planes propuestos para los riesgos identificados y definidos como riesgos mitigables.

3.2. Fase I Contexto de la organización

La Universidad es una institución de educación superior de carácter privado, con un tamaño pequeño, cuenta con alrededor de 45 empleados entre administrativos y docentes a tiempo completo, 64 docentes a tiempo parcial y un promedio de 600 alumnos. Tiene alrededor de 10 años de funcionamiento y cuenta con una sede única ubicada en la ciudad de Quito.

Actualmente la institución está trabajando en el establecimiento de un Sistema de Calidad bajo la norma ISO 9001, para lo que se encuentra definiendo sus procesos, debido se considera importante trabajar también en el diseño de un Sistema de Gestión de seguridad de la Información, que complemente el Sistema de Calidad.

Una vez realizado el análisis previo del estado actual de la Universidad en el apartado 2.4 del capítulo 2, se evidencia que la seguridad de la información en la institución está en una fase inicial, que cuenta con procesos definidos y algunos procedimientos documentados, por otro lado, no cuenta con políticas ni normativas en esta área, sin embargo, las autoridades apoyan las iniciativas para el diseño del proyecto del SGSI.

3.2.1. Misión

Según la página oficial, La Universidad Iberoamericana del Ecuador su misión es "*una institución de educación superior con orientación humanística, que forma profesionales con valores éticos; comprometida a fomentar el desarrollo sostenible del país a través de la investigación, la tecnología y la innovación*".

3.2.2. Objetivos estratégicos

El SGSI debe alinearse con los objetivos estratégicos de la Universidad, siendo los fundamentales para la seguridad de la información los siguientes (UNIBE, 2019):

- Orientar la acción estratégica institucional a partir de un Modelo de Gestión Académico-Administrativo, que establezca con claridad los procesos y líneas de acción a seguir de cara a los desafíos que le impone una universidad del siglo XXI.

- Fortalecer la gestión del personal académico a fin de que responda a los requerimientos de calidad de la formación que se imparte en las carreras universitarias La Universidad

promoverá la utilización de las nuevas tecnologías de información y comunicación en los procesos académico-administrativos de la institución.

- Fortalecer la gestión administrativo-financiera institucional para garantizar la calidad de los procesos administrativos.

- Fortalecer el Sistema de información académico-administrativa a fin de mejorar los procesos internos y responder con eficiencia los requerimientos de los organismos de control.

- Mantener los planes de innovación tecnológica que la Universidad viene implementando para contribuir al mejoramiento de los servicios ofertados a estudiantes y comunidad universitaria en general.

3.2.4. Estructura de la Universidad

Como todas las instituciones de educación superior las tres principales áreas de la Universidad son; la formación docente, la investigación y la vinculación con la sociedad. La Figura 19 muestra el organigrama de la Universidad, en el cual puede apreciarse las distintas direcciones y las áreas en las que está dividida.

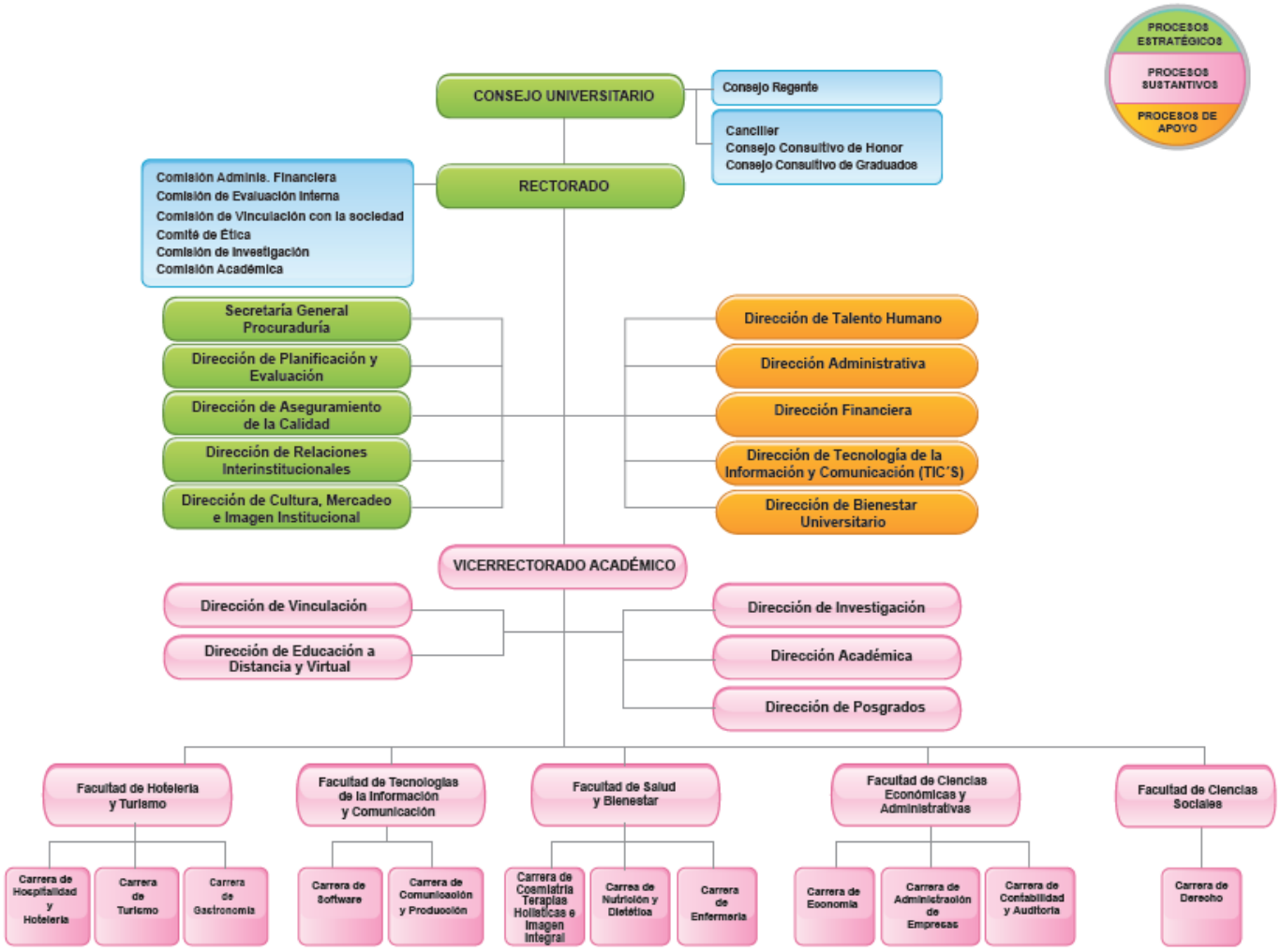


Figura 20. Organigrama de la Universidad

Fuente: (UNIBE, 2019)

En la Tabla 10 se puede observar los roles administrativos que influirán en la aprobación y establecimiento de criterios para la implementación del SGSI.

Tabla 10. Roles administrativos para el SGSI

ROL	CARACTERÍSTICAS
Consejo Universitario	Máximo órgano rector de la Universidad conformado por las autoridades de la institución y representantes de los docentes, empleados y estudiantes.
Rector	Máxima autoridad de la Universidad
Comisión Académica	Comisión nombrada para revisar aspectos académicos de la institución
Director Académico	Encargado del proceso de la Gestión Académica
Director Financiero	Encargado del proceso de la Gestión Financiera
Director de Talento Humano	Encargado del proceso de la Gestión de Talento Humano
Director TIC	Encargado del proceso de la Gestión de la Tecnología de la Información y Comunicación
Comité de Seguridad de la Información	No existe al momento un responsable de aprobar las normas y procedimientos de seguridad de la información
Oficial de Seguridad de la Información	No existe al momento un responsable de ejecutar las políticas, normas y procedimientos de seguridad de la información

Fuente: Elaboración propia

3.3. Fase II Liderazgo

La segunda parte del SGSI en la norma ISO/IEC 27001 establece el liderazgo de la alta dirección, es decir las autoridades de la institución, que deben manifestar su apoyo al proyecto con actividades como determinar los objetivos que se pretenden alcanzar con la implementación del SGSI, aprobar las Políticas Generales de Seguridad de la Información, definir los roles y responsabilidades del personal en relación a la seguridad de la información, entre otros.

3.3.1. Alcance

La cláusula 4.5 de la norma ISO 27001, establece que la organización determinará los límites o el alcance del sistema de gestión de la seguridad de la información. De acuerdo con esto, las autoridades han determinado el alcance del SGSI en la UNIB.E a los procesos:

Gestión Académica, Financiera, Talento Humano y TIC, debido a que estos son los procesos que manejan la mayor parte de los sistemas de información de la institución, que determinan sus objetivos de negocio. La Tabla 11 muestra una descripción de cada proceso.

Tabla 11. Descripción de Procesos

PROCESO DE LA INSTITUCIÓN	DESCRIPCIÓN
Gestión Académica	Gestión todo lo relacionado los procesos fundamentales de la Universidad, es la encargada de la admisión, oferta académica, calificaciones, vida estudiantil, documentación docente y estudiantil. Utiliza un sistema Académico para cumplir sus funciones
Gestión Financiera	Gestiona, los datos de clientes y proveedores, lleva el manejo financiero de la Universidad, realiza el cumplimiento de las obligaciones fiscales. Utiliza un sistema Financiero/Contable.
Gestión de Talento Humano	Se encarga de la gestión de nóminas y contratos del personal. La gestión de esta información se realiza mediante un Sistema de Talento humano.
Gestión de Tecnología de la Información y Comunicación	Se encarga de la infraestructura tecnológica y de telecomunicaciones de la Universidad y la instalación, mantenimiento y gestión los sistemas de información

Fuente: Elaboración propia

3.3.2. Objetivos del SGSI

Los objetivos de seguridad propuestos para el SGSI son los siguientes:

- Mejorar la seguridad de la información en la institución a través de implantar controles que logren aumentar la disponibilidad de datos y la confidencialidad de los mismos, a través de las actividades asociadas a las áreas académicas, recursos humanos y TIC.
- Mantener un registro y respuesta adecuada a incidentes y amenazas a la seguridad de la información.
- Mejorar la imagen frente a los clientes y entidades reguladoras al mejorar el manejo de la información en los procesos de la institución

- Optimizar el presupuesto destinado a las TIC con respecto a los proyectos de seguridad de la información.

- Crear políticas de seguridad adecuadas para la institución, que deberá ser acatada por todos los trabajadores para mantener en todo momento la seguridad de la información.

Estos objetivos de seguridad deben ser revisado y aprobados por parte de las autoridades de la institución.

3.3.3. Política General de Seguridad de la Información.

La Política de seguridad de la información, es un documento de alto nivel, general, que debe ser aprobado por las autoridades de la institución y debe ser conocido por toda la comunidad universitaria, además debe estar siempre disponible para consulta, por lo cual será colocado en la Intranet de la institución.

Para la realización de la Política de Seguridad de la Información se ha tomado en cuenta los dominios de seguridad que establece el Anexo A de la norma ISO/IEC 27001. Esta política será presentada para la revisión y aprobación por parte de las autoridades. A continuación, se presenta los lineamientos de dicha política:

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN - UNIB.E

I. Introducción

La Universidad Iberoamericana del Ecuador – UNIB.E considera que la información debe ser protegida en todo momento ya que es un activo muy importante para su funcionamiento diario y para ayudarle a cumplir con sus objetivos estratégicos. Las políticas, normas y procedimientos de Seguridad de la Información permitirán proteger dicha información de diversas amenazas que puedan presentarse, garantizando así la continuidad de los sistemas de información que la institución maneja, minimizando los riesgos a los que está expuesta.

II. Alcance

La propuesta permitirá gestionar adecuadamente la seguridad de la información en la institución. Para ello, se debe aplicar a toda la institución universitaria socializad con todos los trabajadores de la misma para sui estricto cumplimento.

III. Objetivo

Proteger los activos de información de la UNIB.E, frente a cualquier tipo de amenazas sean estas internas o externas, naturales, accidentales o deliberadas, para asegurar niveles adecuados de confidencialidad, integridad y disponibilidad de la información, garantizando el funcionamiento adecuado de sus sistemas de información.

Para lo cual se establecen las siguientes normas y procedimientos de acuerdo con los requisitos de la UNIB.E y el marco legal aplicable.

IV. Definiciones

Activo de información. – Información o sistema que permiten el tratamiento de ésta y que tiene valor para la institución.
Autenticidad. - Garantizar el origen de la transacción, validando la fuente de información para evitar suplantación de identidad.

Confidencialidad. – Imposibilidad de que las personas, o procesos no autorizados tengan acceso a la información.

Disponibilidad. - Acceso y utilización de la información en el momento que ésta es requerida.

Evaluación de Riesgos. - Análisis de las amenazas y vulnerabilidades que pueden afectar a los activos de información, la probabilidad de que ocurran esas amenazas y el impacto en el adecuado funcionamiento de la institución.

Incidente de Seguridad. - Evento que afecte la seguridad de la información inesperado o no deseado y que afecte el normal desarrollo de los procesos.

Información. - Activo de la institución, estos pueden ser documentos tanto físicos como digitales, datos, equipos, personas, instalaciones, etc.

Integridad. - Exactitud en la información a la que se accede.

Propietario de la Información. – Persona o proceso responsable de clasificar la información de acuerdo los criterios dados de integridad, confiabilidad y disponibilidad, definir los acceso y permisos para cada usuario de acuerdo con sus funciones.

Seguridad de la Información. – Preservación de la confidencialidad, integridad y

disponibilidad de la información.

V. Organización de la seguridad de la información

a) La coordinación de la Gestión de la Seguridad de la Información en la Institución estará a cargo de un comité técnico, que deberá incluir a todo el personal universitario. Este comité deberá reunirse de manera periódica, dejando registros de todos los encuentros realizados.

c) El director de Talento Humano será responsable de comunicar al personal de la Universidad, sus obligaciones respecto del cumplimiento de las Políticas de Seguridad de la Información y tendrá a su cargo la capacitación y socialización de esta política.

d) Los directores de Carrera serán los encargados de comunicar a los docentes y estudiantes a su cargo las obligaciones del cumplimiento de estas políticas.

e) Los propietarios de Información tendrán la responsabilidad de clasificar la información, mantener actualizada la misma y definir los accesos a los usuarios de acuerdo con sus funciones y competencia.

f) Oficial de seguridad de la información, debe ser nombrado por el comité de Seguridad de la Información, y será responsable de llevar a cabo la implementación de las medidas de seguridad seleccionadas, detectar necesidades de capacitación y mantener actualizados los elementos que dan soporte al SGSI.

VI. Activos de información

a) La información debe clasificarse en base a la importancia que tiene para los procesos de la UNIB.E y también de acuerdo con su valor monetario, otro factor que puede determinar su clasificación son los requisitos legales y que tan sensible es el activo en cuanto a la integridad, disponibilidad y confiabilidad. Adicionalmente debe etiquetarse todos los activos de información. Se deberán establecer un procedimiento denominado “Clasificación y etiquetado de Información”, que regule esta tarea.

b) La Dirección de TIC deberá seleccionar las herramientas tecnológicas que faciliten la tarea de inventario y clasificación de los activos de información.

c) Se deberán establecer normas y procedimientos para el manejo de la información contenida en cualquier medio, físico o electrónico.

VII.- Recurso humano

a) La Dirección de Talento Humano deberá incluir en sus procedimientos la planificación y administración del capital humano, con el fin de prevenir riesgos de error humano, robo, fraude, uso inadecuado de los recursos, etc.

b) Se deberá establecer los términos y condiciones de los contratos de trabajo estableciendo responsabilidades del personal en cuanto a la seguridad de la información, durante y después de la relación laboral con la UNIBE.

c) Todo el personal de la UNIBE deberá recibir periódicamente una adecuada capacitación y concientización en temas de seguridad de la información tales como: normativa vigente, procedimientos de seguridad, respuesta a incidentes de seguridad, las responsabilidades legales y el correcto uso de la tecnología y los sistemas de información.

d) Deberá ser responsabilidad y obligación del personal de la UNIBE asistir a los cursos o talleres de capacitación en seguridad de la información, presencial o virtual, registrar su asistencia y rendir la evaluación correspondiente.

e) Los estudiantes deben conocer y aceptar en cada matrícula el acuerdo de uso de los recursos tecnológicos.

f) El reglamento de estudiantes deberá contemplar sanciones disciplinarias para los incidentes de seguridad y mal uso de recursos tecnológicos.

VIII.- Seguridad física

a) El cuarto de servidores deberá tener un acceso controlado y restringido únicamente a personal autorizado, para lo cual la Dirección de TIC elaborará normas y procedimientos para el control y registro del acceso a dicha área.

b) Los servidores institucionales deberán localizarse en un ambiente seguro y protegido, que tenga en cuenta el control de acceso, seguridad física, aire acondicionado, UPS y sistemas de detección de incendios.

c) Se deberá contar con un plan de mantenimiento periódico para el equipamiento que asegure su disponibilidad e integridad.

d) Los equipos de escritorio deben instalarse de manera que estén seguros contra robo o alteración y debe capacitarse al personal de la Universidad para un uso adecuado del equipo.

e) Ningún activo de información podrá ser retirado de las instalaciones de la UNIBE sin autorización.

f) Las copias de seguridad deben conservarse de forma adecuada para lo cual se deberá contar con normas y procedimiento que deberán ser elaborados por la Dirección de TIC.

g) Todas las áreas de la Universidad tienen la responsabilidad de manejo de forma adecuada sus copias individuales de seguridad.

IX.- Comunicaciones y operaciones

a) La Dirección de TIC deberá establecer normas, procedimientos y responsabilidades para gestionar y operar los recursos tecnológicos y mantener un control de cambios en los sistemas y equipos.

b) Se deberá revisar periódicamente la capacidad de procesamiento instalada y se tomarán acciones oportunas a fin de garantizar que no se supere la capacidad de procesamiento y almacenamiento adecuados, que cubran la demanda requerida presente y futura.

c) Se deberán determinar controles de detección y prevención contra malware e intrusiones. Los computadores de la Universidad deberán contar con software antivirus y mantenerlos siempre actualizados. A los usuarios no se les permitirá desinstalar ni cambiar este software.

d) Se deberá contar con un procedimiento de respaldo de equipos, datos y software esencial, que incluyan, forma de conservación, pruebas de restablecimiento oportuno y el registro de eventos y fallas.

e) Los respaldos de la información de cada empleado de la institución deberá ser responsabilidad de estos. Esta copia deberá entregarse al Departamento de TIC para su registro y custodia.

f) La Dirección de TIC en conjunto con el Comité de Seguridad de la Información deberá establecer un procedimiento para el uso correcto de Internet y correo electrónico.

g) Los medios removibles de almacenamiento (flash, discos externos, tarjetas de memoria, etc.) deberán ser controlados y protegidos contra daño, robo, acceso y utilización no autorizados, con el fin de impedir pérdida de información e interrupción de las actividades de la UNIB.E.

h) Cualquier instalación de software en los equipos de la Universidad debe ser aprobada por el Departamento de TIC, no se permitirá la instalación de software que no tenga licencia adquirida de forma legal. El Departamento de TIC deberá desinstalar cualquier software ilegal.

i) Los sistemas de información deberán estar configurados para permitir el registro de las actividades de los usuarios, y cualquier evento de seguridad de la información.

X.- Control de acceso

a) Deberán determinarse perfiles de acceso a los sistemas de información institucionales restringiendo el acceso necesario para realizar sus funciones, estos perfiles deber ser determinados por los propietarios de los activos de información.

b) Las claves de administrador de los sistemas deberán ser mantenidas en un lugar seguro por la Dirección de TIC y deberán ser cambiadas en intervalos regulares de tiempo.

c) El acceso a los servicios de red a través de redes inalámbricas deberá sujetarse a los lineamientos que para el efecto defina la Dirección de TIC acorde a las políticas definidas por el Comité de Seguridad de la Información.

d) Deberán existir medidas para el control de equipos de usuario desatendidos y fomentar la cultura de escritorios limpios, para lo cual se crearán procedimientos que serán socializados con el personal de la institución.

XI.- Incidentes de la seguridad de la información

a) El Comité de Seguridad de la Información deberá desarrollar un procedimiento formal para gestionar los eventos de seguridad de la información, definiendo mecanismos de reporte, recolección de evidencias, manejo y respuesta ante el incidente, responsabilidades y lecciones aprendidas.

XII.- Revisión y actualización

a) El Comité de Seguridad de la Información deberá revisar y actualizar la Política de Seguridad de la Información anualmente o cuando sea necesario por un cambio legal, operativo o tecnológico, etc. que afecte su normal ejecución y cumplimiento.

XIII.- Sanciones

a) El personal de la UNIBE que incumpla esta Política de Seguridad de la Información deberá ser sancionado de acuerdo con lo establecido en las disposiciones internas emitidas por la máxima autoridad de la Universidad, siguiendo el debido proceso.

3.3.4. Definición de roles y responsabilidades

La definición de roles y responsabilidades debe ser aprobada por las máximas autoridades de la Universidad. Para el presente trabajo se han definido los siguientes roles tomando en cuenta lo que la norma aconseja y el tamaño de la institución:

a) Autoridades

Las mismas deberán definir el alcance, definir los objetivos y aprobar la política de seguridad diseñada en la institución. Igualmente es responsabilidad de las autoridades ofrecer los recursos para lograr un buen funcionamiento del sistema implantado, asignar roles y responsabilidades dentro del sistema, sociabilizar las políticas implantadas y formar parte del Comité de seguridad.

b) Comité de Seguridad de la información

Se conformará una comisión técnica denominada Comité de Seguridad de la Información compuesta por: Director Académico o su delegado, Director Administrativo o su delegado, Director de Talento Humano, Director de Tecnología de la Información y Comunicación, Oficial de Seguridad de la Información.

Esta comisión deberá coordinar la Gestión de la Seguridad de la Información incluyendo la colaboración y contribución del personal de toda la institución.

c) Oficial de Seguridad de la Información

Será responsable de velar por la efectiva implantación de las medidas de seguridad seleccionadas, detectar necesidades de capacitación y emprender las acciones adecuadas,

mantener actualizados los elementos que dan soporte al SGSI.

d) Propietario de la información

Estarán a cargo de clasificar la información según el nivel de sensibilidad y criticidad de esta. Además, deberá realizar la documentación y determinar los permisos para el acceso de los usuarios según sus funciones y competencias.

e) Responsable de Talento Humano

El responsable de la Dirección de Talento Humano será responsable de comunicar a todo el personal que labora en la Universidad, las obligaciones respecto del cumplimiento de las Políticas de Seguridad de la Información y tendrá a su cargo la suscripción de un acuerdo con los términos y condiciones sobre el uso de los recursos de TI.

f) Responsable de tecnología

Implantar las medidas de seguridad seleccionadas para mitigar los riesgos. Supervisar el funcionamiento de los activos de información y de las medidas de seguridad aplicadas sobre los mismos.

g) Decanos y directores de carrera

Los decanos y directores de carrera serán los encargados de comunicar a los docentes y estudiantes a su cargo las obligaciones del cumplimiento de estas políticas.

h) Personal

Las responsabilidades de los demás miembros del personal de la UNIB.E son: conocer y cumplir los términos establecidos en la política de seguridad, notificar las incidencias de seguridad de la información al oficial de seguridad de la información.

Esta definición de roles y responsabilidades será presentada en un documento para la revisión y aprobación por parte de las autoridades de la Universidad.

3.4. Fase III Planificación: Gestión de riesgos de la información

En esta fase se realiza la gestión de riesgos, se define la metodología que se utilizará para este procedimiento, ésta incluye el inventario de los activos de información, la valoración de

los activos, la detección de vulnerabilidades, amenazas y riesgos que pueden sufrir dichos activos en los procesos que están dentro del alcance del SGSI y el tratamiento de estos. Para recolectar la información se aplicaron las técnicas de entrevistas a los usuarios de los sistemas y a los responsables de los procesos y la observación directa.

3.4.1. Metodología de la gestión de riesgos de la seguridad de la información

La metodología para la gestión de riesgos propuesta y utilizada en el presente trabajo se basa en la norma IEC/ISO 27005 adaptada al contexto de la UNIB.E. La metodología de gestión de riesgos propuesta para la institución tiene las siguientes actividades:

a) Realizar un inventario de activos de información en los procesos dentro del alcance del SGSI.

b) Valorar los activos de información de la Universidad en cuanto a su impacto en la seguridad de la información (confiabilidad, integridad y disponibilidad).

c) Determinar las amenazas y vulnerabilidades de cada activo y valorar la probabilidad de ocurrencia de las amenazas y el impacto en la seguridad.

d) Con esta evaluación determinar la manera de tratar los riesgos encontrados.

3.4.2. Inventario de activos de información

De acuerdo con el alcance definido para el SGSI se realizó un inventario de los activos de información en los procesos Académico, Financiero, Talento Humano y TIC, según la norma ISO/IEC 27005 los activos de información pueden ser: primarios y de soporte, en los primarios están las actividades y procesos y la información (documentos y datos) y en los de soporte están el hardware, software, redes, personas, sitios, organización.

El inventario de activos de información se realizó con los responsables de los procesos y usuarios que manejan información en las áreas que están dentro del alcance del SGSI. Los resultados de dicho inventario se indican en la Tabla 12, este inventario incluye el nombre del activo, una breve descripción de este, el tipo de activo según lo estipula la norma y el soporte en el que se almacena.

Tabla 12. Inventario de Activos de Información

Nombre del activo	Descripción del activo	Tipo	Soporte	Propietario del activo
1. ACADÉMICO				
Admisión	Proceso de admisión de los aspirantes para el ingreso	Proceso	digital	Secretario/a Académico
Matriculación	Formalizar la vinculación de los estudiantes en los programas académicos.	Proceso	digital	Director de carrera
Ejecución académica	Proceso de ejecución académica garantizando su planificación, evaluación y seguimiento.	Proceso	físico	Director Académico
Titulación	Procedimientos para la obtención del título universitario	Proceso	físico/digital	Secretario/a Académico
Ficha de inscripción	Registro de los datos personales de los aspirantes	Información	digital	Secretario/a Académico
Actas de grado	Creación de actas de grado	Información	físico/digital	Secretario/a Académico
Récord académico	listado de asignaturas y calificaciones de los niveles cursados por los estudiantes	Información	digital	Secretario/a Académico
Calificaciones	Cuadro de calificaciones	Información	digital	Secretario/a Académico
Promociones de calificaciones	Libreta de calificaciones	Información	digital	Secretario/a Académico
Certificados de matrícula	Constancia de la matrícula	Información	digital	Secretario/a Académico
Carpeta del estudiante	Capeta de documentos personales y académicos del estudiante	Información	físico	Secretario/a Académico
Portafolio del docente	Capeta con información de los cursos impartidos y los resultados de evaluación	Información	físico	Director Académico
Certificado de Egresamiento	Certificado que refleja la condición de egresado de la carrera	Información	físico	Secretario/a Académico
Registro de calificaciones sistemáticas	Ficha de calificaciones de los estudiantes por parciales	Información	físico	Secretario/a Académico
Registro de calificaciones totales	Ficha de calificaciones de los estudiantes por parciales	Información	digital	Docente

Nombre del activo	Descripción del activo	Tipo	Soporte	Propietario del activo
Distributivos de docentes	Listado de docentes y la asignatura que dicta	Información	digital	Secretario/a Académico
POA	Plan Operativo Anual del área	Información	digital	Director de Carrera
Horarios docentes	Horarios planificados para los docentes de las carreras	Información	digital	Director de Carrera
Informe de homologación	Asignaturas aprobadas para estudiantes externos o por cambio de carrera	Información	físico/digital	Director de Carrera
Autorizaciones estudiantes	Autorización para exámenes atrasados, matrícula extraordinaria, etc.	Información	físico	Director de Carrera
Memorandos, oficios	Comunicación interna	Información	físico	Decano
Evaluación docente	Evaluación por parte de estudiantes, pares y directivos.	Información	digital	Director Académico
Evaluación ingreso de docentes	Evaluación a docentes aspirantes a cargos.	Información	físico	Decano
Lista de asistencia	Lista de estudiantes con su asistencia.	Información	físico	Docente
Acta de reuniones	Informe de las reuniones	Información	físico	Director Académico
Syllabus y Planes analíticos	Guías para la docencia	Información	digital	Docente
Exámenes	Resultado de la evaluación al estudiante	Información	físico/digital	Docente
Horarios de clases	Documento con la carga horaria	Información	digital	Director de Carrera
Carga académica	Asignaturas tomadas por el estudiante, generado al momento de la matrícula	Información	físico/digital	Director de Carrera
Becas	Postulación, calificación y asignación de becas	Proceso	físico	Director Bienestar
Informes anuales	Informes de gestión y resultados	Información	físico/digital	Directores
Planificación anual	POA departamental	Información	digital	Directores
Solicitudes de estudiantes	Formulario de solicitud e informe de aprobación o negación	Información	físico	Decanos
Reglamentos	Reglamentos de la Universidad	Información	físico/digital	Director Académico
Aprobación temas de tesis	Informe de aprobación de temas de tesis.	Información	físico	Director de Carrera
Calendario académico	Documento de fechas académicas	Información	digital	Director Académico

Nombre del activo	Descripción del activo	Tipo	Soporte	Propietario del activo
Convenios de prácticas	Documento de Convenios con instituciones externas	Información	físico	Decanos
Sistema Académico	Sistema de la Gestión académica	Software	digital	Director Académico
Secretario académico	Realiza los procesos académicos	Personal	No aplica	No aplica
2. FINANCIERO				
Facturación	Realizar la facturación de servicios	Proceso	digital	Auxiliar contable
Declaración de impuestos	Realizar la declaración de impuestos	Proceso	digital	Auxiliar contable
Reportes financieros contables	Emitir los estados financieros y reportes contables	Proceso	digital	Director Financiero
Pago de nómina	Generación de pagos de compromisos laborales	Proceso	digital	Director Financiero
Sistema Financiero	Sistema Financiero/Contable	Software	digital	Director Financiero
Facturas compras	Compras realizadas	Información	físico/digital	Auxiliar contable
Facturas servicios	Facturas a estudiantes	Información	físico/digital	Auxiliar contable
Retenciones	Documento de retenciones en la fuente	Información	físico	Auxiliar contable
Anexos SRI	Información pago impuestos	Información	digital	Auxiliar contable
Diarios tarjetas de crédito	Informe de uso de tarjetas de crédito	Información	físico/digital	Auxiliar contable
Análisis cuentas	Informe financiero	Información	digital	Director Financiero
Lista de deudores	Lista de estudiantes con atraso en los pagos	Información	digital	Auxiliar contable
Reporte de ventas	Informe financiero	Información	digital	Auxiliar contable
Facturas de ventas	Facturas emitidas por cobro de pensiones y tasas a estudiantes	Información	digital	Auxiliar contable
Balances	Informe financiero	Información	digital	Director Financiero
Reporte proveedores	Informe financiero	Información	digital	Director Financiero
Nómina	Pago a empleados	Información	digital	Director Financiero
Presupuesto	Informe financiero	Información	digital	Director Financiero
Reporte cuentas por cobrar	Informe financiero	Información	digital	Director Financiero
Impuestos	Información para pago de impuestos	Información	digital	Director Financiero
Contadora	Realiza los procesos financieros	personal	No aplica	No aplica
3. TALENTO HUMANO				

Nombre del activo	Descripción del activo	Tipo	Soporte	Propietario del activo
Contratar personal	Selección y contratación de personal	Proceso	físico	Director Talento Humano
Personal		Proceso	digital	Director Talento Humano
Contratos	Documento del contrato de trabajo	Información	físico/digital	Director Talento Humano
Avisos IESS	Avisos de entrada, salida, cambios, etc. del personal	Información	físico/digital	Director Talento Humano
Memorandos, oficios	Comunicación interna	Información	físico/digital	Director Talento Humano
Files del personal	Carpeta con la información y certificados de los empleados y docentes a tiempo parcial	Información	físico	Director Talento Humano
Sistema Lince Web	Software de Talento Humano	Software	digital	Director Talento Humano
Certificados laborales	Documentos de certificados de trabajo	Información	físico	Director Talento Humano
Director Talento Humano	Realiza los procesos de Talento Humano	personal	No aplica	No aplica
4. TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN				
Administrar infraestructura tecnológica	Administración de la Infraestructura tecnológica	Proceso	físico/digital	Director TIC
Soporte a usuarios	Recibir, atender y dar seguimiento a las solicitudes de soporte	Proceso	físico/digital	Director TIC
Resoluciones de cambios académicos	Resoluciones de Procuraduría	Información	físico	Director TIC
Solicitudes de soporte técnico	Pedido de soporte técnico	Información	digital	Director TIC
Servidor Aplicaciones	Equipo de cómputo	Hardware	no aplica	Director TIC
Repositorio	Equipo de cómputo	Hardware	no aplica	Director TIC
Computadores fijos	Equipo de cómputo	Hardware	no aplica	Director TIC
Portátiles	Equipo de cómputo	Hardware	no aplica	Director TIC
Windows Server 2012	Licencia de uso	Software	digital	Director TIC
Base de datos	Datos de aplicaciones	Software	digital	Director TIC
Página Web	Portal informativo y de consulta	Software	digital	Director TIC
Antivirus	Software antivirus, antispam	Software	digital	Director TIC
Moodle	Plataforma de eLearning	Software	digital	Director TIC
Correo Electrónico	Correo institucional	Software	digital	Director TIC
Firewall	Equipo de seguridad	Red	no aplica	Director TIC
Switch	Equipo de comunicación	Red	no aplica	Director TIC

Nombre del activo	Descripción del activo	Tipo	Soporte	Propietario del activo
Servicio de Internet	Servicio de comunicación	Sitio	no aplica	Director TIC
Director TIC	Realiza los procesos de TIC	personal	No aplica	No aplica

Fuente: Elaboración propia

3.4.3. Valoración de Activos

El siguiente paso a la identificación de los activos de información es la valoración de los activos identificados, para lo cual se debe elegir la escala que se va a utilizar y los criterios para la asignación de ese valor. Para valorar los activos se considera el costo de la pérdida de confidencialidad, integridad y disponibilidad cuando se presente un incidente de seguridad, esto de acuerdo con el criterio de los usuarios y responsables de los activos y del director de TIC. Los criterios para la valoración se definen en la Tabla 13, considerando las recomendaciones de la norma ISO/IEC 27005. Se ha elegido un rango de valores del 1 al 5 donde el 1 representa un muy bajo impacto y el 5 un muy alto impacto.

Tabla 13. Criterios de impacto

Valor	Criterio	Consideración	Total
1	Insignificante	No afecta el trabajo normal ni produce pérdidas financieras o de reputación a de la institución.	1-3
2	Bajo impacto	Afecta el trabajo normal pero no produce pérdidas financieras o de reputación a de la institución.	4-6
3	Medio impacto	Afecta el trabajo normal y puede producir pérdidas financieras o de reputación a de la institución	7-9
4	Alto impacto	Afecta el trabajo normal, produce pérdidas financieras o de reputación a de la institución e incumplimiento de obligaciones legales.	10-12
5	Crítico	Afecta el trabajo normal, produce grandes pérdidas financieras y de reputación, pérdida de credibilidad en sistemas de información internos, incapacidad para cumplir las obligaciones legales	13-15

Fuente: Adaptado norma ISO 27005

De acuerdo con los criterios definidos en la Tabla 13, se procedió a realiza la valoración de los activos en el inventario previamente realizado. Definiéndose el total de la valoración como la suma aritmética de los valores asignados para confidencialidad, integridad y disponibilidad, adicionalmente se asignó colores en un mapa de calor sobre el valor total, con esto se logró determinar cuáles activos tienen mayor impacto en la seguridad de la información para la institución. Esta valoración se indica en la Tabla 14.

Tabla 14. Valoración de activos

Nombre del activo	Confidencialidad	Integridad	Disponibilidad	Total
1. ACADÉMICO				
Admisión	2	5	4	11
Matriculación	2	5	4	11
Ejecución académica	2	5	3	10
Titulación	2	5	2	9
Ficha de inscripción	4	5	4	13
Actas de grado	1	5	1	7
Récord académico	4	5	5	14
Promociones de calificaciones	1	5	2	8
Certificados de matrícula	1	2	1	4
Carpeta del estudiante	5	5	5	15
Portafolio del docente	2	5	2	9
Certificado de Egresamiento	1	4	1	6
Registro de calificaciones sistemáticas	3	4	1	8
Registro de calificaciones totales	2	5	5	12
Distributivos de docentes	1	3	2	6
POA	1	3	2	6
Horarios docentes	1	3	2	6
Informe de homologación	1	2	1	4
Autorizaciones estudiantes	1	4	3	8
Memorandos, oficios	1	3	1	4
Evaluación docente	2	5	3	10
Evaluación ingreso de docentes	2	5	3	10
Lista de asistencia	2	5	3	10
Acta de reuniones	2	5	2	9
Syllabus y Planes analíticos	1	3	2	6
Exámenes	1	5	3	9
Horarios de clases	1	4	3	8
Carga académica	1	5	2	8
Becas	3	5	3	11
Informes anuales	1	5	2	8
Planificación anual	1	5	2	8
Solicitudes de estudiantes	1	1	2	4

Nombre del activo	Confidencialidad	Integridad	Disponibilidad	Total
Reglamentos	2	4	3	9
Aprobación temas de tesis	1	2	2	5
Calendario académico	1	5	2	8
Convenios de prácticas	1	5	3	9
Sistema Académico	5	5	5	15
Secretario académico	2	4	4	11
2. FINANCIERO				
Facturación	2	5	4	11
Declaración de impuestos	2	5	4	11
Reportes financieros contables	3	5	4	12
Pago de nómina	4	5	4	13
Sistema Financiero	5	5	5	15
Facturas compras	1	5	2	8
Facturas servicios	1	5	2	8
Retenciones	1	5	5	11
Anexos SRI	1	5	3	9
Diarios tarjetas de crédito	1	5	3	9
Análisis cuentas	3	5	4	12
Lista de deudores	1	3	3	7
Reporte de ventas	1	5	2	8
Facturas de ventas	2	5	2	9
Balances	3	5	3	11
Reporte proveedores	1	5	2	8
Nómina	4	5	5	14
Presupuesto	1	5	3	9
Reporte cuentas por cobrar	2	5	2	9
Impuestos	4	5	5	14
Contadora	3	4	4	11
3. TALENTO HUMANO				
Contratar personal	2	3	3	8
Personal	4	5	4	14
Contratos	4	5	5	14
Avisos IESS	2	5	5	12
Memorandos, oficios	2	5	2	9

Nombre del activo	Confidencialidad	Integridad	Disponibilidad	Total
Files del personal	5	5	5	15
Sistema Lince Web	3	5	3	11
Certificados laborales	1	3	1	5
Director Talento Humano	3	4	4	11
4. TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN				
Administrar infraestructura tecnológica	4	5	5	14
Soporte a usuarios	2	3	4	9
Resoluciones de cambios académicos	2	5	3	10
Solicitudes de soporte técnico	1	3	2	6
Servidor Aplicaciones	5	5	5	15
Repositorio	5	5	5	15
Computadores fijos	3	5	4	12
Portátiles	2	3	3	8
Windows Server 2012	5	5	5	15
Base de datos	5	5	5	15
Página Web	5	5	5	15
Antivirus	2	3	5	10
Moodle	2	4	3	9
Correo Electrónico	2	5	5	12
Firewall	5	5	5	15
Switch	0	5	5	10
Servicio de Internet	2	3	4	9
Director TIC	3	4	4	11

Fuente: Elaboración propia

Después de la valoración de los activos de información se puede determinar aquellos activos que son vitales para la institución o que pueden afectar su desempeño o producir pérdidas financieras, de servicios, de reputación o pueden afectar la evaluación de los organismos de control del estado.

Se ha definido que sobre aquellos activos que tengan color rojo claro y rojo oscuro en el mapa de calor se realice el proceso de análisis de riesgos.

3.4.4. Determinar amenazas y vulnerabilidades de los activos

Como tercer paso se realizó el análisis de las amenazas y vulnerabilidades que pueden dar origen a los riesgos en los activos de información considerando la probabilidad de ocurrencia de un riesgo y el impacto que tendría sobre las 3 características de la seguridad de la información: disponibilidad, confidencialidad e integridad en los activos de información.

Para la evaluación de las amenazas y vulnerabilidades se parte de tablas de amenazas y vulnerabilidades conocidas, que están disponibles en diferentes fuentes, la norma ISO/IEC 27005 cuenta con una tabla de ejemplo, esta tabla se incluye en el Anexo C, también se puede incluir aquellas amenazas y vulnerabilidades que el equipo de trabajo considere oportuno por experiencias de sucesos anteriores. En general las amenazas pueden ser deliberadas, accidentales o del ambiente (naturales), en la Tabla 15 se puede observar algunos ejemplos de amenazas. Los métodos de evaluación de vulnerabilidades pueden incluir actividades como: entrevistas, encuestas, observación directa y revisión de documentos.

Tabla 15. Ejemplos de Amenazas

TIPO	AMENAZA
Deliberadas	Malware
	Denegación de Servicio
	Alteración de Información
	Destrucción de Información
	Fugas de Información
	Acceso no autorizado a la Información
	Suplantación de Identidad
	Abuso de privilegios de acceso
	Interceptación de información
	Manipulación de programas
	Ingeniería Social
	Manipulación de configuraciones
Naturales	Terremotos
	Erupción Volcánica
Accidentales	Corte de Suministro eléctrico
	Condiciones inadecuadas de temperatura o humedad
	Errores de mantenimiento/actualización
	Agotamiento de recursos

TIPO	AMENAZA
	Indisponibilidad del personal
	Fallo de servicios de comunicaciones
	Interrupción de servicios de soporte
	Errores de usuarios
	Errores de administrador
	Errores de configuración
	Incendios

Fuente: Adaptado de la Norma ISO/IEC 27005

Para la valoración del riesgo se toma la probabilidad de ocurrencia del riesgo y el impacto en caso de que este se produzca, el cálculo del riesgo se lo puede realizar de varias maneras, para esta metodología se ha definido que se lo calculará multiplicando la probabilidad por el impacto.

$$riesgo = impacto \ + \ probabilidad$$

Los valores elegidos para la probabilidad de ocurrencia de un riesgo responden a una escala del 1 al 5 donde 5 representa la máxima probabilidad y 1 la mínima probabilidad, estos valores se indican en la Tabla 16.

Tabla 16. Probabilidad que ocurra la amenaza

Valor	Probabilidad	Frecuencia
1	Poco probable	Riesgo mínimamente probable
2	Improbable	Riesgo que se puede producir eventualmente
3	Moderado	Riesgo que se presenta de manera moderada.
4	Probable	Riesgo que puede producir habitualmente
5	Muy probable	Riesgo que se produce recurrentemente

Fuente: Adaptado Norma 27005

La valoración del impacto depende de las consecuencias que tendrían para la institución que el riesgo se produzca, la Tabla 17 en cambio presenta la valoración definida para el nivel de impacto que tendría sobre el activo si el riesgo se produjera.

Tabla 17. Impacto de ocurrencia de un riesgo

Valor	Criterio	Consideración
1	Insignificante	No afecta el trabajo normal ni produce pérdidas financieras o de reputación a de la institución.
2	Bajo impacto	Afecta el trabajo normal pero no produce pérdidas financieras o de reputación a de la institución.
3	Medio impacto	Afecta el trabajo normal y puede producir pérdidas financieras o de reputación a de la institución
4	Alto impacto	Afecta el trabajo normal, produce pérdidas financieras o de reputación a de la institución e incumplimiento de obligaciones legales.
5	Crítico	Afecta el trabajo normal, produce grandes pérdidas financieras y de reputación, pérdida de credibilidad en sistemas de información internos, incapacidad para cumplir las obligaciones legales

Fuente: Adaptado Norma 27005

La Tabla 18 muestra el resultado de la valoración del riesgo para los activos críticos, basado en un listado de amenazas y vulnerabilidades comunes y en la definición de los valores de probabilidad y de impacto.

Tabla 18. Valoración del riesgo en los activos de información

Activo	Tipo	Amenaza	Propietario riesgo	Vulnerabilidades	Probabilidad	Impacto	Riesgo
Servidor Aplicaciones	Hardware	Interrupción de servicio	TIC	Mantenimiento insuficiente Instalación fallida de los medios de almacenamiento	3	5	8
		Destrucción de equipos o medios.	TIC	Ausencia de esquemas de reemplazo periódico	3	5	8
		Robo de equipos	TIC	Almacenamiento sin protección Copia no controlada	1	5	6
		Error en el uso	TIC	Ausencia de un eficiente control de cambios en la configuración	2	5	7
Repositorio	Hardware	Interrupción de servicio	TIC	Mantenimiento insuficiente Instalación fallida de los medios de almacenamiento	3	3	6
		Destrucción de equipos o medios.	TIC	Ausencia de esquemas de reemplazo periódico	3	3	6
		Robo de equipos	TIC	Almacenamiento sin protección Copia no controlada	1	3	4

Activo	Tipo	Amenaza	Propietario riesgo	Vulnerabilidades	Probabilidad	Impacto	Riesgo
		Error en el uso	TIC	Ausencia de un eficiente control de cambios en la configuración	1	3	4
Computadores fijos	Hardware	Interrupción de servicio	TIC	Mantenimiento insuficiente Ataque de Virus, malware	4	3	7
		Destrucción de equipos o medios.	TIC	Ausencia de esquemas de reemplazo periódico	3	3	6
		Abuso de privilegios de acceso	TIC	Contraseñas inseguras	2	3	5
		Robo de equipos	TIC	Almacenamiento sin protección Copia no controlada	3	3	6
Ficha de inscripción	Información	Acceso no autorizado	ACAD	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	2	3	5
		Abuso de derechos	ACAD	Dejar sesión abierta cuando se ausenta del equipo. Asignación errada de los derechos de acceso	2	3	5
		Mal funcionamiento del software	ACAD	Ausencia de control de cambios eficaz	2	3	5
Récord académico	Información	Acceso no autorizado	ACAD	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	2	5	7
		Abuso de derechos	ACAD	Dejar sesión abierta cuando se ausenta del equipo. Asignación errada de los derechos de acceso	2	5	7
		Mal funcionamiento del software	ACAD	Ausencia de control de cambios eficaz	2	5	7
Carpeta del estudiante	Información	Acceso no autorizado	ACAD	No están almacenadas de manera adecuada	2	5	7
		Fuego, inundación	ACAD	Falta de condiciones físicas y de respaldo de la información	2	5	7
Registro de calificaciones totales	Información	Acceso no autorizado	ACAD	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	2	5	7
		Abuso de derechos	ACAD	Dejar sesión abierta cuando se ausenta del equipo. Asignación errada de los derechos de acceso	2	5	7
		Mal funcionamiento del software	ACAD	Ausencia de control de cambios eficaz	2	5	7

Activo	Tipo	Amenaza	Propietario riesgo	Vulnerabilidades	Probabilidad	Impacto	Riesgo
Evaluación docente	Información	Acceso no autorizado	ACAD	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	2	3	5
		Abuso de derechos	ACAD	Dejar sesión abierta cuando se ausenta del equipo. Asignación errada de los derechos de acceso	2	3	5
		Mal funcionamiento del software	ACAD	Ausencia de control de cambios eficaz	1	3	4
Evaluación ingreso de docentes	Información	Acceso no autorizado	ACAD	No están almacenadas de manera adecuada	1	3	4
		Fuego, inundación	ACAD	Falta de condiciones físicas y de respaldo de la información	1	3	4
Lista de asistencia	Información	Acceso no autorizado	ACAD	No están almacenadas de manera adecuada	1	3	4
		Fuego, inundación	ACAD	Falta de condiciones físicas y de respaldo de la información	1	3	4
Becas	Información	Acceso no autorizado	ACAD	No están almacenadas de manera adecuada	1	5	6
		Fuego, inundación	ACAD	Falta de condiciones físicas y de respaldo de la información	1	5	6
		Cambio no autorizado de información	ACAD	Falla en el control acceso físico	1	5	6
Retenciones	Información	Acceso no autorizado	FIN	No están almacenadas de manera adecuada	2	4	6
		Fuego, inundación	FIN	Falta de condiciones físicas y de respaldo de la información	2	4	6
Análisis cuentas	Información	Abuso de derechos	FIN	Disposición o reutilización de equipos sin borrado adecuado	2	3	5
		Mal funcionamiento del software	FIN	Ausencia de control de cambios eficaz	2	3	5
Balances	Información	Acceso no autorizado	FIN	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	2	4	6
		Abuso de derechos	FIN	Dejar sesión abierta cuando se ausenta del equipo. Asignación errada de los derechos de acceso	2	4	6

Activo	Tipo	Amenaza	Propietario riesgo	Vulnerabilidades	Probabilidad	Impacto	Riesgo
		Mal funcionamiento del software	FIN	Ausencia de control de cambios eficaz	1	4	5
Nómina	Información	Acceso no autorizado	FIN	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	2	5	7
		Abuso de derechos	FIN	Dejar sesión abierta cuando se ausenta del equipo. Asignación errada de los derechos de acceso	2	5	7
		Mal funcionamiento del software	FIN	Ausencia de control de cambios eficaz	2	5	7
Impuestos	Información	Acceso no autorizado	FIN	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	2	4	6
		Abuso de derechos	FIN	Dejar sesión abierta cuando se ausenta del equipo. Asignación errada de los derechos de acceso	2	4	6
		Mal funcionamiento del software	FIN	Ausencia de control de cambios eficaz	1	4	5
Avisos IESS	Información	Acceso no autorizado	TH	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	2	3	5
		Abuso de derechos	TH	Dejar sesión abierta cuando se ausenta del equipo. Asignación errada de los derechos de acceso	2	3	5
		Mal funcionamiento del software	TH	Ausencia de control de cambios eficaz	1	3	4
Files del personal	Información	Acceso no autorizado	TH	No están almacenadas de manera adecuada	3	5	5
		Fuego, inundación	TH	Falta de condiciones físicas y de respaldo de la información	2	5	7
		Cambio no autorizado de información	TH	Falla en el control acceso físico	3	5	5
Resoluciones de cambios académicos	Información	Acceso no autorizado	TIC	No están almacenadas de manera adecuada	2	5	5
		Fuego, inundación	TIC	Falta de condiciones físicas y de respaldo de la información	2	5	7
		Cambio no autorizado de información	TIC	Falla en el control acceso físico	1	5	6

Activo	Tipo	Amenaza	Propietario riesgo	Vulnerabilidades	Probabilidad	Impacto	Riesgo
Contadora	persona	Error al ingresar datos	FIN	Falta de conciencia acerca de la seguridad	2	5	7
		Incumplimiento en la disponibilidad del personal	FIN	Ausencia del personal	2	5	7
Director Talento Humano	persona	Error al ingresar datos	TH	Falta de conciencia acerca de la seguridad	2	5	7
		Incumplimiento en la disponibilidad del personal	TH	Ausencia del personal	2	5	7
Director TIC	persona	Incumplimiento en la disponibilidad del personal	TH	Ausencia del personal	2	5	7
		Destrucción de equipos y medios	TIC	Procedimientos inadecuados de contratación	2	5	7
Secretario académico	persona	Error al ingresar datos	ACAD	Falta de capacitación Desmotivación del personal	2	5	7
		Incumplimiento en la disponibilidad del personal	ACAD	Ausencia del personal	2	5	7
Firewall	Red	Interrupción de servicio	TIC	Falta de mantenimiento de equipos Configuración inadecuada, cambios sin control	3	5	8
		Cambios no autorizados en configuración	TIC	Falta de procedimiento de control de cambios. Asignación inadecuada de roles y permisos. Falta de respaldos de información	2	5	7
Switch	Red	Fallas del equipo de telecomunicaciones	TIC	Conexión deficiente de los cables. Punto único de fallas	3	5	8
		Saturación del Sistema de Información	TIC	Gestión inadecuada de la red	3	5	8
		Espionaje remoto	TIC	Arquitectura insegura de la red	2	5	7
Sistema Académico	Software	Instalación de software no autorizado	TIC	Descarga y uso no controlado de software. Ausencia de copias de respaldo	2	5	7
		Falsificación de derechos	TIC	Ausencia de mecanismos de identificación y autentificación de usuario. Gestión deficiente de las contraseñas.	3	5	8

Activo	Tipo	Amenaza	Propietario riesgo	Vulnerabilidades	Probabilidad	Impacto	Riesgo
		Manipulación con software	TIC	Ausencia de copias de respaldo	3	5	8
Sistema Financiero	Software	Instalación de software no autorizado	TIC	Descarga y uso no controlado de software. Ausencia de copias de respaldo	2	5	7
		Falsificación de derechos	TIC	Ausencia de mecanismos de identificación y autentificación de usuario. Gestión deficiente de las contraseñas.	3	5	8
		Manipulación con software	TIC	Ausencia de copias de respaldo	3	5	8
Sistema Lince Web	Software	Instalación de software no autorizado	TIC	Descarga y uso no controlado de software. Ausencia de copias de respaldo	2	4	6
		Falsificación de derechos	TIC	Ausencia de mecanismos de identificación y autentificación de usuario. Gestión deficiente de las contraseñas.	2	4	6
		Manipulación con software	TIC	Ausencia de copias de respaldo	2	4	6
Windows Server 2012	Software	Abuso de derechos	TIC	Asignación errada de los derechos de acceso	2	5	7
		Procesamiento ilegal de datos	TIC	Habilitación de servicios innecesarios	2	5	7
		Mal funcionamiento del software	TIC	Ausencia de control de cambios eficaz	2	5	7
Base de datos	Software	Procesamiento ilegal de datos	TIC	Habilitación de servicios innecesarios	2	5	7
		Falsificación de derechos	TIC	Ausencia de mecanismos de identificación y autentificación de usuario. Gestión deficiente de las contraseñas.	3	5	8
		Mal funcionamiento del software	TIC	Ausencia de control de cambios eficaz	3	5	8
		Error en uso	TIC	Configuración incorrecta de parámetros	3	5	8
Página Web	Software	Abuso de derechos	TIC	Asignación errada de los derechos de acceso	2	3	5
		Procesamiento ilegal de datos	TIC	Habilitación de servicios innecesarios	3	3	6
		Mal funcionamiento del software	TIC	Ausencia de control de cambios eficaz	2	3	5

Activo	Tipo	Amenaza	Propietario riesgo	Vulnerabilidades	Probabilidad	Impacto	Riesgo
Antivirus	Software	Instalación de software no autorizado	TIC	Descarga y uso no controlado de software	3	3	6
Correo Electrónico	Software	Instalación de software no autorizado	TIC	Falta políticas y normas de seguridad Inadecuada asignación de roles y permisos Falta de control para instalación de software	2	4	6
		Spam	TIC	Falta de software de seguridad. Mala configuración del servicio	3	4	7
		Suplantación de identidad de usuarios	TIC	Contraseñas no seguras Ausencia o inadecuada plataforma de vigilancia física Inadecuado mecanismo de cifrado	3	4	7

Fuente: Elaboración propia

3.4.5. Tratamiento del riesgo

El tratamiento del riesgo permite decidir la manera de actuar frente a los riesgos analizados, las opciones de tratamiento de riesgos son:

- Retener o aceptar el riesgo: En este caso en caso de ocurrir el riesgo se aceptará sin realizar ninguna acción, ya que los costos de eliminarlos podrían ser mayores a los que origina el riesgo.
- Reducir el riesgo: para minimizarlo, en este caso se tomarán accione para reducir la probabilidad de que el riesgo se produzca.
- Evitar el riesgo: Si es posible se eliminarán las actividades que puedan producir el riesgo.
- Transferir el riesgo: Traspasar el riesgo a terceros como pueden ser: empresas aseguradoras, realizar outsourcing, etc.

Se debe definir los criterios con los que va a trabajar, teniendo en cuenta las limitaciones que se puedan presentar tanto financieras, legales, etc. Para la Universidad la decisión de tratamiento de riesgos se ha definido en base a los criterios indicados en la Tabla 19.

Tabla 19. Decisiones de tratamiento del riesgo

1 – 3	Mínimo	Asumir el riesgo
4 – 5	Bajo	Reducir el riesgo
6 – 8	Medio	Reducir o evitar el riesgo
9 - 10	Alto	Transferir el riesgo

Fuente: Adaptado Noma ISO 27705

Con esta decisión de tratamiento de riesgos se puede ver que para los riesgos que están en un nivel alto o medio se deben realizar acciones a corto o mediano tiempo para minimizar su ocurrencia, para los riesgos con un nivel bajo pueden realizarse acciones en un tiempo más largo. Los riesgos con un nivel mínimo serán aceptados por la institución.

3.5. Fase IV Documentación del SGSI

3.5.1. Declaración de Aplicabilidad

La Declaración de aplicabilidad muestra los controles de la norma ISO/IEC 27002 y del Anexo A de la ISO/IEC 27001 que son relevantes para el SGSI de la Universidad y que permiten adicionalmente mitigar los riesgos encontrados en la etapa de análisis de riesgos, permite también verificar que se han considerado todos los controles previstos en la norma.

Se incluye la justificación de la selección de algunos controles, estas razones pueden ser:
L: Requerimiento Legal: requisitos legales, reglamentarios o regulatorios.

C: Obligaciones contractuales: por la prestación de servicios.

N: Requerimiento del negocio; necesidades de seguridad de la institución.

R: Análisis de riesgos: resultado del análisis de riesgos.

La declaración de aplicabilidad se muestra en la Tabla 20.

Tabla 20. Declaración de aplicabilidad

Categoría de control	Objetivo de control / control	Control existente	Control planteado	Razones			
				L	C	N	R
Políticas de Seguridad	Dirección de la alta gerencia para la seguridad de la información						
	Políticas de seguridad de la información	ninguno	Definir, aprobar y socializar políticas de seguridad			x	x
	Revisión de las políticas de seguridad de la información	ninguno	Revisión anual de las políticas de seguridad			x	
Organización de la Seguridad de la Información	Organización interna						
	Roles y responsabilidad de seguridad de la información	ninguno	Definir y aprobar roles y responsabilidades			x	x
	Segregación de deberes	ninguno	Definir y aprobar roles y responsabilidades			x	
	Contacto con autoridades	ninguno	Definir y aprobar roles y responsabilidades			x	
	Contacto con grupos de interés especial	ninguno	Definir y aprobar roles y responsabilidades			x	
	Seguridad de la información en la gestión de proyectos	ninguno	Definir y aprobar roles y responsabilidades			x	
	Dispositivos móviles y teletrabajo						
	Política de dispositivos móviles	ninguno	Definir procedimiento para el control y acceso de dispositivos móviles			x	
	Teletrabajo	ninguno	No aplica, no existe el teletrabajo en la institución				
Seguridad en los Recursos Humanos	Previo al empleo						
	Verificación de antecedentes	Existe procedimiento	Revisión del procedimiento existente			x	
	Términos y condiciones del empleo	Existe procedimiento	Definir acuerdo de confidencialidad	x		x	
	Durante el empleo						
	Responsabilidades de la Alta Gerencia	Existe procedimiento	Ninguno				
	Conciencia, educación y entrenamiento de seguridad de la información	ninguno	Definir plan de capacitación y concientización de la seguridad de la información			x	

Categoría de control	Objetivo de control / control	Control existente	Control planteado	Razones			
				L	C	N	R
	Proceso disciplinario	ninguno	Definir sanciones para empleados que incumplan las políticas de seguridad			x	
	Terminación y cambio de empleo						
	Termino de responsabilidades o cambio de empleo	ninguno	Talento Humano y el área Administrativa serán responsables de verificar que los activos sean devueltos.				
Gestión de Activos	Responsabilidad de los activos						
	Inventario de activos	ninguno	Reporte periódico del inventario de activos			x	
	Propiedad de activos	ninguno	En el inventario de activos se define el responsable de los activos			x	
	Uso aceptable de los activos	ninguno	Definir el procedimiento de uso aceptable de activos			x	
	Devolución de activos	ninguno	Definir el procedimiento para la devolución de activos			x	
	Clasificación de la información						
	Clasificación de la información	Procedimiento existe en área Académica	Definir un sistema de clasificación de la información general			x	
	Etiquetado de la información	Procedimiento existe en área Académica	Definir un sistema de etiquetado de la información general			x	
	Manejo de activos	ninguno	Definir el procedimiento para el manejo activos			x	x
	Manejo de medios						
	Gestión de medios removibles	ninguno	Definir el procedimiento para la devolución de activos			x	
	Eliminación de medios	ninguno	Definir el procedimiento para la eliminación de medios			x	
	Transporte de medios físicos	ninguno	No aplica, no se realiza transporte de medios físicos				
Control de Acceso	Requerimientos de negocio para el control de acceso						
	Política de control de acceso	Procedimiento Ad hoc	Documentar y cumplir el procedimiento de control de acceso			x	x

Categoría de control	Objetivo de control / control	Control existente	Control planteado	Razones			
				L	C	N	R
	Acceso a redes y servicios de red	Procedimiento Ad hoc	Procedimiento de uso de Internet y correo electrónico			x	x
	Gestión de accesos de usuario						
	Registro y baja del usuario	Procedimiento Ad hoc	Definir el procedimiento para registro y baja de usuarios			x	x
	Provisión de acceso a usuarios	Procedimiento Ad hoc	Documentar y cumplir el procedimiento de control de acceso			x	x
	Gestión de derechos de acceso privilegiados	Procedimiento Ad hoc	Documentar y cumplir el procedimiento de control de acceso			x	x
	Gestión de información de autenticación secreta de usuarios	Ninguno	Ninguno, para esta etapa no se va a considerar este control				
	Revisión de derechos de acceso de usuarios	Procedimiento Ad hoc	Definir el procedimiento para la devolución de activos			x	x
	Eliminación o ajuste de derechos de acceso	Procedimiento Ad hoc	Definir el procedimiento para la devolución de activos			x	x
	Responsabilidades del usuario						
	Uso de información de autenticación secreta	ninguno	Ninguno, para esta etapa no se va a considerar este control				
	Control de acceso de sistemas y aplicaciones						
	Restricción de acceso a la información	Procedimiento Ad hoc	Documentar y cumplir el procedimiento de control de acceso		x	x	
	Procedimientos de inicio de sesión seguro	Procedimiento Ad hoc	Documentar y cumplir el procedimiento de control de acceso		x	x	
	Sistema de gestión de contraseñas	Procedimiento Ad hoc	Documentar y cumplir el procedimiento de control de acceso		x	x	
	Uso de programas y utilidades privilegiadas	ninguno	No aplica				
	Control de acceso al código fuente del programa	ninguno	No aplica, no se realiza desarrollo de software				
Criptografía	Controles criptográficos						

Categoría de control	Objetivo de control / control	Control existente	Control planteado	Razones			
				L	C	N	R
	Política en el uso de controles criptográficos	Ninguno	Ninguno, para esta etapa no se va a considerar este control				
	Gestión de llaves	Ninguno	Ninguno, para esta etapa no se va a considerar este control				
Seguridad Física y del Entorno	Áreas seguras						
	Perímetro de seguridad físico	Existe control mediante CCTV	Revisión de las medidas de acceso físico y seguridad.		x	x	x
	Controles físicos de entrada	Existe control de ingreso por torno, CCTV	Revisión de las medidas de acceso físico y seguridad.		x	x	x
	Seguridad de oficinas, habitaciones y facilidades	CCTV	Revisión de las medidas de acceso físico y seguridad.		x	x	x
	Protección contra amenazas externas y del ambiente	Existen sensores, extintores, etc.	Revisión de las medidas de acceso físico y seguridad.		x	x	x
	Trabajo en áreas seguras	Ninguno	Definición de áreas seguras			x	x
	Áreas de entrega y carga	Ninguno	No aplica				
	Equipo						
	Instalación y protección de equipo	Procedimiento Ad hoc	Definir y cumplir procedimiento para instalación segura de equipos.			x	x
	Servicios de soporte	Existe				x	x
	Seguridad en el cableado	Existe	Revisión y actualización de cableado estructurado			x	x
	Mantenimiento de equipos	Existe plan de mantenimiento	Actualización y cumplimiento del plan de mantenimiento	x		x	x
	Retiro de activos	Procedimiento Ad hoc	Definir y cumplir procedimiento para retiro de equipos.			x	
	Seguridad del equipo y activos fuera de las instalaciones	Ninguno	Ninguno, no existen activos fuera de las instalaciones				
	Eliminación segura o reuso del equipo	Procedimiento Ad hoc	Definir el procedimiento eliminación y reuso			x	x
	Equipo de usuario desatendido	Ninguno	Política y generar cultura de cierre de sesiones y uso de contraseña			x	x

Categoría de control	Objetivo de control / control	Control existente	Control planteado	Razones			
				L	C	N	R
	Política de escritorio limpio y pantalla limpia	Ninguno	Política y generar cultura de escritorio limpio			x	x
Seguridad en las Operaciones	Procedimientos Operacionales y Responsabilidades						
	Documentación de procedimientos operacionales	Ninguno	Ninguno, para esta etapa no se va a considerar este control				
	Gestión de cambios	Ninguno	El control de cambios de los sistemas de información			x	x
	Gestión de la capacidad	Ninguno	Ninguno, para esta etapa no se va a considerar este control			x	x
	Separación de los ambientes de desarrollo, pruebas y operación	Ninguno	No aplica, no se realiza desarrollo de software				
	Protección de Software Malicioso						
	Controles contra software malicioso	Existe, software antivirus y antimalware	Concientización del personal sobre evitar actividades peligrosas			x	x
	Respaldo						
	Respaldo de información	Existe procedimiento para realizar respaldos	Automatizar proceso de respaldo de información		x	x	x
	Bitácoras y monitoreo						
	Bitácoras de eventos	ninguno	Procedimiento de revisión de logs			x	
	Protección de información en bitácoras	ninguno	Respaldo de información de logs			x	
	Bitácoras de administrador y operador	Procedimiento Ad hoc	Procedimiento de revisión de logs			x	
	Sincronización de relojes	ninguno	ninguno				
	Control de software operacional						
	Instalación de software en sistemas operacionales	ninguno	Procedimiento de revisión de logs			x	x
	Gestión de vulnerabilidades técnicas						
	Gestión de vulnerabilidades técnicas	ninguno	Procedimiento de revisión de logs			x	x
	Restricciones en la instalación de software	ninguno	Revisión y actualización de cableado estructurado			x	x
	Consideraciones de auditoria de sistemas de información						

Categoría de control	Objetivo de control / control	Control existente	Control planteado	Razones			
				L	C	N	R
	Controles de auditoría de sistemas de información	ninguno	Ninguno, para esta etapa no se va a considerar este control				x
Seguridad en las Comunicaciones	Gestión de seguridad en red						
	Controles de red	Procedimiento Ad hoc	Adquirir y configurar software de monitoreo de red			x	x
	Seguridad en los servicios en red	Firewall, IPS, antispam	Ninguno			x	x
	Segregación en redes	Existe segregación de redes	Revisar y optimizar la segregación de redes			x	x
	Transferencia de información						
	Políticas y procedimientos para la transferencia de información	Ninguno	Ninguno, para esta etapa no se va a considerar este control				
	Acuerdos en la transferencia de información	Ninguno	Ninguno, para esta etapa no se va a considerar este control				
	Mensajería electrónica	Ninguno	Ninguno, para esta etapa no se va a considerar este control				
	Acuerdos de confidencialidad o no-revelación	Ninguno	Ninguno, para esta etapa no se va a considerar este control				
Adquisición, Desarrollo y Mantenimiento de Sistemas	Requerimientos de seguridad en sistemas de información						
	Análisis y especificación de requerimientos de seguridad	Ninguno	Ninguno, para esta etapa no se va a considerar este control				
	Aseguramiento de servicios de aplicación en redes públicas	Ninguno	Ninguno, para esta etapa no se va a considerar este control				
	Protección de transacciones en servicios de aplicación	Ninguno	Ninguno, para esta etapa no se va a considerar este control				
	Seguridad en el proceso de desarrollo y soporte						
	Política de desarrollo seguro	Ninguno	No aplica, no se realiza desarrollo de software				
	Procedimientos de control de cambios del sistema	Ninguno	No aplica, no se realiza desarrollo de software				
	Revisión técnica de aplicaciones después de	Ninguno	No aplica, no se realiza desarrollo de software				

Categoría de control	Objetivo de control / control	Control existente	Control planteado	Razones			
				L	C	N	R
	cambios a la plataforma operativa						
	Restricción de cambios en paquetes de software	Ninguno	No aplica, no se realiza desarrollo de software				
	Principios de seguridad en la ingeniería de sistemas	Ninguno	No aplica, no se realiza desarrollo de software				
	Entorno de desarrollo seguro	Ninguno	No aplica, no se realiza desarrollo de software				
	Desarrollo tercerizado	Ninguno	Ninguno, para esta etapa no se va a considerar este control				
	Pruebas de seguridad del sistema	Ninguno	Ninguno, para esta etapa no se va a considerar este control				
	Pruebas de aceptación del sistema	Ninguno	Ninguno, para esta etapa no se va a considerar este control				
	Datos de prueba						
	Protección de datos de prueba	Ninguno	Ninguno, para esta etapa no se va a considerar este control				
Relaciones con Proveedores	Seguridad de la información en relaciones con el proveedor						
	Política de seguridad de la información en las relaciones con el proveedor	Ninguno	Ninguno, para esta etapa no se va a considerar este control				
	Atención de tópicos de seguridad en los acuerdos con el proveedor	Ninguno	Ninguno, para esta etapa no se va a considerar este control				
	Cadena de suministros de tecnologías de la información y comunicaciones	Ninguno	Ninguno, para esta etapa no se va a considerar este control				
	Gestión de entrega de servicios de proveedor						
	Monitoreo y revisión de servicios del proveedor	Ninguno	Ninguno, para esta etapa no se va a considerar este control				
	Gestión de cambios a los servicios del proveedor	Ninguno	Ninguno, para esta etapa no se va a considerar este control				
	Gestión de incidentes de seguridad de la información y mejoras						

Categoría de control	Objetivo de control / control	Control existente	Control planteado	Razones			
				L	C	N	R
Gestión de Incidentes de Seguridad de la Información	Responsabilidades y procedimientos	Ninguno	Procedimiento de gestión de incidentes de seguridad de la información			x	
	Reporte de eventos de seguridad de la información	Ninguno	Procedimiento de gestión de incidentes de seguridad de la información			x	
	Reporte de debilidades de seguridad de la información	Ninguno	Procedimiento de gestión de incidentes de seguridad de la información			x	
	Valoración y decisión de eventos de seguridad de la información	Ninguno	Procedimiento de gestión de incidentes de seguridad de la información			x	
	Respuesta a incidentes de seguridad de la información	Ninguno	Procedimiento de gestión de incidentes de seguridad de la información			x	
	Aprendizaje de incidentes de seguridad de la información	Ninguno	Procedimiento de gestión de incidentes de seguridad de la información			x	
	Colección de evidencia	Ninguno	Procedimiento de gestión de incidentes de seguridad de la información			x	
Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio	Continuidad de la seguridad de la información						
	Planeación de la continuidad de la seguridad de la información	Ninguno	Ninguno, para esta etapa no se va a considerar este control				
	Implementación de la continuidad de la seguridad de la información	Ninguno	Ninguno, para esta etapa no se va a considerar este control				
	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Ninguno	Ninguno, para esta etapa no se va a considerar este control				
	Redundancias						
	Disponibilidad de facilidades de procesamiento de información	Ninguno	Ninguno, para esta etapa no se va a considerar este control				
Cumplimiento	Cumplimiento con Requerimientos Legales y Contractuales						
	Identificación de legislación aplicable y requerimientos contractuales	Ninguno	Ninguno, para esta etapa no se va a considerar este control				

Categoría de control	Objetivo de control / control	Control existente	Control planteado	Razones			
				L	C	N	R
	Derechos de propiedad intelectual (IPR)	Ninguno	Procedimiento para cumplir la ley de Derechos de Propiedad Intelectual,	x		x	
	Protección de registros	Ninguno	Ninguno, para esta etapa no se va a considerar este control				
	Privacidad y protección de información personal identificable (PIR)	Ninguno	Ninguno, para esta etapa no se va a considerar este control				
	Regulación de controles criptográficos	Ninguno	No aplica				
	Revisiones de seguridad de la información						
	Revisión independiente de seguridad de la información	Ninguno	Ninguno, para esta etapa no se va a considerar este control				
	Cumplimiento con políticas y estándares de seguridad	Ninguno	Ninguno, para esta etapa no se va a considerar este control				
	Revisión del cumplimiento técnico	Ninguno	Ninguno, para esta etapa no se va a considerar este control				

Fuente: Elaboración propia, en base a la norma ISO/IEC 27002

3.5.2. Plan de tratamiento del riesgo

En base a la declaración de aplicabilidad se establece un plan de tratamiento de riesgos que define proyectos de mitigación de riesgos. Estos proyectos tienen que ver con los objetivos y el alcance del SGSI y también con limitaciones financieras, de acuerdo con estos criterios se definen los siguientes proyectos que se muestran en la Tabla 21 tomando en cuenta el período de un año.

Tabla 21. Plan de Tratamiento de riesgos

DESCRIPCIÓN DEL PLAN DE TRATAMIENTO					
No.	**PROYECTO**	**DESCRIPCIÓN**	**RESPONSABLE**	**DURACIÓN**	**FECHA INICIO**
1	Política de Seguridad de la Información	Definición, aprobación y socialización de la Política de Seguridad	Comité de Seguridad	30 días	Por definir
2	Roles de seguridad	Definición de roles y responsabilidades	Autoridades	15 días	Por definir

3	Control de dispositivos móviles	Definir procedimiento para el control y acceso de dispositivos móviles	TIC	15 días	Por definir
4	Contratación de personal	Revisión de procedimiento para comprobar antecedentes del candidato	Talento Humano	10 días	Por definir
5	Capacitación y concienciación del SGSI	Definir e implementar plan de capacitación y concientización de la seguridad de la información	Talento Humano	60 días	Por definir
6	Sanciones sobre incidentes de seguridad	Definir sanciones para empleados que incumplan las políticas de seguridad	Talento Humano	15 días	Por definir
7	Uso aceptable de activos	Definir el procedimiento de uso aceptable de activos	Oficial de seguridad	15 días	Por definir
8	Devolución de activos	Definir el procedimiento para la devolución de activos	Oficial de seguridad	15 días	Por definir
9	Control de acceso	Definir el procedimiento para el control de acceso a los Sistemas de información	TIC	10 días	Por definir
10	Política de Contraseñas	Definir el procedimiento para la generación y uso de contraseñas seguras y su cambio periódico.	TIC	10 días	Por definir
11	Respaldo de información	Adquisición de software y equipo para respaldo automático de información	TIC	60 días	Por definir
12	Control de cambios en la configuración	Definir procedimiento de control de cambios en la configuración	TIC	15 días	Por definir
13	Mantenimiento preventivo	Definir y hacer seguimiento al nuevo plan de mantenimiento preventivo	TIC	45 días	Por definir
14	Contraseñas no seguras	Definir plan de capacitación y concienciación de uso de contraseñas seguras	TIC	30 días	Por definir
15	Gestión de incidentes de seguridad de la información	Definir el procedimiento de gestión de incidentes de seguridad de la información	Comité de Seguridad	15 días	Por definir
16	Cableado estructurado	Revisión y actualización del cableado estructurado	TIC	90 días	Por definir

Fuente: Elaboración propia

El plan de tratamiento de riesgos debe ser revisado y aprobado por el Comité de Seguridad de la Información y las autoridades de la Universidad.

3.6. Fase V Plan de Implementación del SGSI

3.6.1. Plan de Implementación del SGSI

A continuación, en la Tabla 22 se presenta el plan de implementación del SGSI, que debe ser aprobado por las autoridades para comenzar con el proyecto.

Tabla 22. Plan de implementación del SGSI

No.	Actividad	Estado	Responsables	Duración
1	Creación de plan de trabajo	Revisión y aprobación	Director TIC, autoridades	Por definir
2	Definición del alcance del SGSI	Revisión y aprobación	Director TIC, autoridades	Por definir
3	Definición de la política de seguridad	Revisión y aprobación	Director TIC, autoridades	Por definir
4	Definición de roles y responsabilidades	Revisión y aprobación	Director TIC, autoridades	Por definir
5	Identificación de los activos de información	Revisión y aprobación	Oficial de Seguridad	Por definir
6	Definición del enfoque del análisis de riesgo	Revisión y aprobación	Comité de Seguridad de la información	Por definir
7	Metodología de análisis de riesgo	Revisión y aprobación	Comité de Seguridad de la información	Por definir
8	Tratamiento de los riesgos	Revisión y aprobación	Comité de Seguridad de la información	Por definir
9	Selección de controles	Revisión y aprobación	Oficial de Seguridad	Por definir
10	Declaración de aplicabilidad	Revisión y aprobación	Oficial de Seguridad	Por definir
11	Planes de tratamiento de riesgo	Revisión y aprobación	Oficial de Seguridad	Por definir
12	Implementación y puesta en marcha de proyectos	Por realizar	TIC, directores de área	Por definir
13	Gestión de los recursos	Por realizar	Comité de Seguridad de la información	Por definir
14	Formación y capacitación	Por realizar	Director de Talento Humano	Por definir
15	Definir conjunto objetivos y métricas	Por realizar	Oficial de Seguridad	Por definir
16	Evaluación del desempeño del SGSI	Por realizar	Auditor interno	Por definir
17	Realizar auditorías internas	Por	Auditor interno	Por definir

		realizar		
18	Revisión por la dirección	Por realizar	Autoridades	Por definir
19	Definir acciones correctivas	Por realizar	Comité de Seguridad de la información	Por definir
20	Plan de mejora continua	Por realizar	Comité de Seguridad de la información, Oficial de Seguridad	Por definir
21	Documentación del SGSI	Por realizar	Oficial de Seguridad	Por definir

Fuente: Elaboración propia

CONCLUSIONES

Las normas internacionales de la familia ISO/IEC 2700 para la seguridad de la información dan un marco referencial para gestionar la seguridad en la UNIB.E, permitiendo de esta manera visibilizar el estado actual de la institución y planear estrategias de cambio y mejora continua en el manejo de la seguridad de la información, definiendo objetivos de seguridad que la Universidad puede alcanzar con un proceso sistemático y documentado.

De acuerdo con el levantamiento de información realizado en la situación actual de la UNIB.E se pudo determinar que actualmente en la institución no existe un Sistema de Gestión de Seguridad, no hay una cultura sobre seguridad de la información y no existen normas ni procedimientos documentados ni aprobados que deban ser de cumplimiento obligatorio en las actividades normales de trabajo de la comunidad universitaria en relación a la seguridad de la información. Sin embargo, la Universidad está trabajando en la descripción y documentación de procesos con la implementación del sistema de calidad, esto hace que por un lado el personal de la institución adquiera ya un conocimiento de la manera en que trabaja un sistema de gestión y al definir los procesos tengan ya una idea más clara de la información que manejan.

Una de las actividades más importantes y complejas del diseño del SGSI es sin duda establecer la metodología de la gestión de riesgos, esta debe involucrar a todas las personas que manejan los sistemas de información de la institución y debe ayudar a visibilizar los riesgos que puede enfrentar la institución, se encontró muchas metodologías definidas para la gestión de riesgos, en el presente trabajo se escogió utilizar una metodología propia que facilite la ejecución de análisis periódicos para mejorar los resultados obtenidos.

El diseño de un Sistema de Seguridad de la Información para la Universidad Iberoamericana del Ecuador, puede ser un gran paso para que la institución aumente su competitividad y mejore la calidad de sus procesos, ya que las organizaciones pequeñas pueden obtener grandes beneficios al tener un marco de referencia en los cuales organizar su planes y proyectos de una manera que se mitiguen los riesgos a los que podría estar expuesta con un desembolso de recursos acorde a su tamaño y necesidades, sin gastos que usualmente no sean necesarios para la Universidad. Además, al tener políticas, normas y procedimientos establecidos y conocidos, las personas que trabajan en la institución van a conocer cómo manejar los activos de información de forma que estén menos expuestos a riesgos de seguridad

y si estos se presentan saber la manera en que deben proceder, para minimizarlos.

Siendo el SGSI un proceso cíclico de mejora continua, debe ser apoyado constantemente, tanto con personal como con presupuesto para que se pueda cumplir con los objetivos de seguridad definidos, este trabajo es un punto de partida que puede ser mejorado cuando de obtenga la retroalimentación de los empleados y autoridades de la institución, una vez que se realice su implementación. Uno de los resultados destacables del análisis realizado a la institución es que, en la fase inicial, el establecimiento de políticas, normas y procedimientos puede marcar una gran diferencia en el resguardo de los activos de información al capacitar y concienciar al personal, y permitir visualizar los objetivos que se quieren alcanzar en cuanto a seguridad.

RECOMENDACIONES

Se debería revisar la norma ISO/IEC 27004 para determinar las métricas que pueden utilizarse para las auditorías tanto internas como externas para medir los resultados una vez que el SGSI esté implementado.

De acuerdo con la situación actual de seguridad de la información en la Universidad se recomienda que el diseño del SGSI propuesto en el presente trabajo se implemente con el alcance definido y luego de ver los resultados se realice un nuevo proyecto extendiéndose al resto de los procesos de manera que la seguridad de la información alcance toda la institución.

En cuanto a la metodología de gestión de riesgos de seguridad de la información, se recomienda la realización de varias interacciones de manera que se evalúe y mejore la metodología propuesta para obtener resultados más precisos que garanticen un mejor control de las amenazas y vulnerabilidades.

Para que el diseño del SGSI propuesto sea implementado con éxito se recomienda que las máximas autoridades de la institución se comprometan activamente en el proceso para que se fomente a todos los niveles de la Universidad una cultura de seguridad de la información.

Se deben realizar charlas y capacitaciones periódicas tanto al inicio del proyecto como durante la implementación, de manera que las personas interioricen los conceptos y la importancia de la seguridad de la información en el cumplimiento de sus labores diarias y en el cumplimento de objetivos institucionales.

BIBLIOGRAFÍA

Alemán Novoa, H., & Rodríguez Barrera, C. (1874). Metodologías para el análisis de riesgos en los SGSI.

Canal, V. (2017). *About O-ISM3*. Recuperado el 30 de enero de 2019, en https://www.ism3.com/node/42.

Carpentier, J. F. (2016). *La seguridad informática en la PYME: Situación actual y mejores prácticas.* Ediciones ENI.

Escrivá, G. G., Romero, S. R. M., & Ramada, D. J. (2013). *Seguridad informática*. Retrieved from https://ebookcentral.proquest.com.

Fernandez, C., & Piattini, M. (2012). *Modelo para el gobierno de las TIC basado en las normas ISO*. AENOR - Asociación Española de Normalización y Certificación. Retrieved from https://ebookcentral.proquest.com.

García Paredes, Y. C. (2015). *Modelo de gestión de la seguridad de información en los procesos críticos de las áreas financieras universitarias. Caso PUCE*. Quito, Tesis de Maestría En Gestión de las Comunicaciones y Tecnologías de la Información

Giménez, A. J. F. (2014). *Seguridad en equipos informáticos*. Retrieved from http://ebookcentral.proquest.com

Gómez, L., & Rivero, P. (2018). *Cómo implantar un SGSI según UNE-ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad,*. Madrid: AENOR - Asociación Española de Normalización y Certificación.

Gómez, F. L., & Andrés, Á. A. (2012). *Guía de aplicación de la norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para PYMES*. Retrieved from http://ebookcentral.proquest.com

González, A., Gallardo, T. F., & Pozo, F. (2017). *Metodología de la Investigación*. Editorial Jurídica del Ecuador.

Haiwen, L., & Graham, K. (2000). BS7799: A suitable model for information security management. *AMCIS 2000 Proceedings*, 142.

Hernández Sampieri, R., & Fernández, L. (2012). *Metodología de la Investigación.* México: McGraw-Hill.

ISO. (2018). Standart ISO/IEC 27000:2018. *Information technology - Security techniques*. ISO.

ISO. (2015). Standart ISO/IEC 27001:2015. *Information technology - Security techniques*. ISO.

ISO. (2017). Standart ISO/IEC 27002:2017. *Information technology - Security techniques*. ISO.

ISO. (2017). Standart ISO/IEC 27005:2017. *Information technology - Security techniques*. ISO.

Kosutic, D. (s.f.). ¿Qué es norma ISO 27001?. Recuperado el 18 de enero de 2019, en https://advisera.com/27001academy/es/que-es-iso-27001/.

Kosutic, D. (2016). *Seguro & Simple: Una guía para la pequeña empresa para la implementación de la ISO 27001 con medios propios*. Advisera.

Ladino, M., Villa, P., & López, A. (2011). Fundamentos de ISO 27001 y su Aplicación en las empresas. *Scienta Et Thecnica*(XVII), 334 - 339.

MHAP, 2012. MAGERIT. *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. - España. Disponible en: http://www.csae.map.es/csi/pg5m20.htm.

MINTEL. (2018). *Libro Blanco de la Sociedad de la Información y del Conocimiento.* Quito: Ministerio de Telecomunicaciones y Sociedad de la Información.

Pallas, G. (20015). *Metodología de Implantación de un SGSI en un grupo empresarial jerárquico.* Montevideo: Tesis de Maestría en ingeniería de Computación.

Parra, A. (2014). *ISO 27001 para PYMES*. Medellín, Tesis de Maestría en Seguridad Informática.

Rifan, M. (2004). *Information security management system (BS7799-2:2002) implementation overview*. Recuperado el 30 de enero de 2019, en https://www.giac.org/paper/gsec/3740/information-security-management-system-bs-7799-2-2002-implementation-overview/105976.

Solarte, F. N. S., Rosero, E. R. E., & Benavides, M. del C. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica - ESPOL*, *28*(5).

(s. a). http://www.iso27000.es/sgsi.html#home. Recuperado el 18 de enero de 2019.

UNIBE. (12 de 2 de 2019). *Universidad Iberoamericana del Ecuador*. Obtenido de https://www.unibe.edu.ec/

Valencia-Duque, F. J., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação, (22), 75-88.*

Vanegas Devia, G., & Pardo, C. (2014). *Hacia un modelo para la gestión de riesgos de TI en MiPyMEs: MOGRIT*.Sistemas & *Telemática*, 12 *(30), 35-48.*

ANEXOS

ANEXO 1
CUESTIONARIO

El presente cuestionario tiene como objetivo realizar un diagnóstico de la cultura institucional sobre la seguridad de la información en la UNIB.E, esto como un primer paso para la implementación de un Sistema de Gestión de Seguridad de la Información en la Universidad, por favor conteste las siguientes preguntas. Muchas gracias por su ayuda.

Directivo		Docente		Administrativo	

1. ¿Sabe o ha escuchado usted qué es la Seguridad de la Información? Si su respuesta es afirmativa describa brevemente qué es para usted la seguridad de la información.

   ____SI ___NO

_____

_____

2. ¿Conoce usted si la UNIBE cuenta con una política de Seguridad de la Información?

   ____SI ___NO

3. ¿Ha recibido capacitación acerca de la importancia de la seguridad de la Información dentro de la UNIBE?

   ____SI ___NO

4. ¿Si existiera un incidente de seguridad de la información, sabe cómo proceder? (pérdida de información, documentos, equipos, etc.)

   ____SI ___NO

5. En su trabajo diario ¿qué tipo de información maneja? (seleccione las que correspondan)

   ☐ interna ☐ externa

   ☐ pública ☐ confidencial

6. ¿Piensa usted que es importante generar dentro de la comunidad universitaria una cultura sobre Seguridad de la Información? ¿Por qué?

   ____SI ___NO

_____

_____

7. ¿Tiene usted identificada la información que utiliza en sus actividades?

____SI ___NO

8. ¿Los procesos en su dirección y/o unidad están claramente definidos?

____SI ___NO

9. ¿Sabe cuál es el tiempo de retención de la información que usted es responsable?

____SI ___NO

10. ¿Sabe usted el procedimiento que hay que seguir para destruir información? Si la respuesta es afirmativa, por favor describa.

____SI ___NO

_____

_____

_____

_____

_____

_____

ANEXO 2
ENTREVISTA

SITUACIÓN ACTUAL ACTIVOS DE INFORMACIÓN

La presente entrevista tiene como objetivo realizar un inventario de información de los activos de información de la UNIB.E, esto como un primer paso de la metodología de gestión de riesgos, por este motivo, se solicita su colaboración llenando los cuadros con la información que maneja en el desarrollo diario de sus funciones. Adicionalmente se solicita que realice un análisis del impacto que tendría para la Universidad el que el activo no esté disponible, se realicen cambios sin autorización o se acceda a él sin autorización. Muchas gracias por su ayuda.

DATOS GENERALES

Nombre:			
Proceso:		Unidad	
		Cargo	

a. Información que usted genera producto de sus actividades.

Nombre	Descripción	Medio (digital, físico)	Tipo (interna, pública, confidencial)	Análisis de impacto en la información		
				Que no esté disponible (alto, medio o bajo)	Por cambio no autorizado (alto, medio o bajo)	Por acceso no autorizado (alto, medio o bajo) (confidencial)

Nombre	Descripción	Medio (digital, físico)	Tipo (interna, pública, confidencial)	Análisis de impacto en la información		
				Que no esté disponible (alto, medio o bajo)	Por cambio no autorizado (alto, medio o bajo)	Por acceso no autorizado (alto, medio o bajo) (confidencial)

b. Información que generan otras personas y que usted utiliza en la ejecución de sus actividades.

Nombre	Descripción	Medio	Responsable de la información

ANEXO 3
LISTADO DE AMENAZAS Y VULNERABILIDADES
Fuente: (ISO/IEC 27005)

Tipo	Amenazas	Origen
Daño físico	Fuego	A, D, E
	Daño por agua	A, D E
	Contaminación	A, D, E
	Accidente importante	A, D, E
	Destrucción del equipo o los medios	A, D, E
	Polvo corrosión congelamiento	A, D, E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológicos	E
	Inundación	E
Pérdida de los servicios esenciales	Falla en el sistema de suministro de agua o de aire acondicionado	A, D
	Pérdida de suministro de energía	A, D, E
	Falla en el equipo de telecomunicaciones	A, D
Perturbación debida a la radiación	Radiación electromagnética	A, D E
	Radiación térmica	A, D, E
	Impulsos electromagnéticos	A, D, E
Compromiso de la información	Interceptación de señales de interferencia comprometedoras	D
	Espionaje remoto	D
	Escucha subrepticia	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	A, D
	Datos provenientes de fuentes no confiables	A D
	Manipulación con hardware	D
	Manipulación con software	A, D
	Detección de la posición	D
Fallas técnicas	Falla del equipo	A
	Mal funcionamiento del equipo	A
	Saturación del sistema de información	A, D
	Mal funcionamiento del software	A
	incumplimiento en el mantenimiento del sistema de información	A, D
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	A, D
	Corrupción de los datos	D
	Procesamiento ilegal de los datos	D

Compromiso de las funciones	Error en el uso	A
	Abuso de derechos	A, D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	A, D, E

Fuente de amenaza	Motivación	Acciones amenazantes
Pirata informático, intruso ilegal	Reto Ego Rebelión Estatus Dinero	• Piratería • Ingeniería social • Intrusión, accesos forzados al sistema • Acceso no autorizado al sistema
Criminal de la computación	Destrucción de información Divulgación ilegal de información Ganancia monetaria Alteración no autorizada de los datos	• Crimen por computador (por ejemplo, espionaje cibernético) • Acto fraudulento (por ejemplo, repetición, personificación, interceptación) • Soborno de la información • Suplantación de identidad • Intrusión en el sistema
Terrorismo	Chantaje Destrucción Explotación Venganza Ganancia política Cubrimiento de los medios de comunicación	• Bomba/terrorismo • Guerra• (warfare) de información • Ataques contra **el** sistema (por ejemplo, negación distribuida del servicio) • Penetración en el sistema • Manipulación del sistema
Espionaje industrial (Inteligencia, empresas, gobiernos extranjeros, otros intereses gubernamentales)	Ventaja competitiva Espionaje económico	• Ventaja de defensa • Ventaja Política • Explotación económica • Hurto de información • Intrusión en laprivacidad personal • Ingeniería social • Penetración en elsistema • Acceso no autorizado al sistema (acceso a información clasificada, de propiedad y/o relacionada con la tecnología)
Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores y omisiones no intencionales) por ejemplo, error en el ingreso de los datos, error de programación)	• Asalto a un empleado • Chantaje • Observar información de • Abuso del computador • negligentes, Venganza • Ingreso de datos falsos o corruptos • Interceptación • Código malintencionado (por ejemplo, virus, bomba lógica, • caballo troyano) • Venta de información personal • Errores (bugs) en el sistema • Sabotaje del sistema • Acceso no autorizado al sistema

ANEXO 4

CARTA DE APOYO INSTITUCIONAL

UNIVERSIDAD TECNOLÓGICA ISRAEL ESCUELA DE POSTGRADOS

MAESTRÍA EN TELEMÁTICA, MENCIÓN: CALIDAD EN EL SERVICIO

(Aprobado por: RPC-SO-19-No.300-2016-CES)

ARTÍCULO

Título:
Aplicación práctica de las normas ISO/IEC 27001 en un sistema de gestión de seguridad de la información para una universidad ecuatoriana
Autor/a:
Ana Cecilia Quintana Arroyo
Tutor/a:
Mg. Henry Rodrigo Vivanco Herrera

APLICACIÓN PRÁCTICA DE LAS NORMAS ISO/IEC 27001 EN UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UNA UNIVERSIDAD ECUATORIANA

Autores: Ing. Ana Cecilia Quintana Arroyo, ac_quintana@yahoo.es
Universidad Iberoamericana del Ecuador, Quito

Mg. Henry Vivanco, hvivanco@uisrael.edu.ec
Universidad Tecnológica Israel, Quito

RESUMEN:

El presente trabajo describe el diseño de un modelo de seguridad de la información para una universidad ecuatoriana basado en las normas ISO 27001. Las mismas que constituyen un referente confiable para la implantación, optimización y administración de procesos dentro de una organización.

El diseño de un Sistema de Seguridad de la Información para una universidad ecuatoriana resulta un avance importante para que dicha institución aumente su competitividad y mejore la calidad de sus procesos.

PALABRAS CLAVE: SGSI, ISO 27001, Modelo de Gestión

ABSTRACT:

This paper describes the design of an information security model for an Ecuadorian university based on the ISO 27001. Standards that constitute a reliable reference for the implementation, optimization and administration of processes within an organization.

The design of an Information Security System for an Ecuadorian university is an important step forward for the institution to increase its competitiveness and improve the quality of its processes.

Keywords: SGSI, ISO 27001, Management Model

I. INTRODUCCIÓN

Los estándares de aceptación general, como son las normas ISO 27001, son un referente confiable para la implantación, optimización y administración de procesos dentro de una organización.

En el caso particular de la institución de educación superior analizada, al momento no dispone de procesos de seguridad de la información, tampoco un modelo de gestión que permita asegurar la información que maneja, siendo esta muy sensible dado que los sistemas de información se maneja tanto las notas como la trayectoria e información personal de los estudiantes y docentes, así como información financiera y de control.

La adopción de un modelo de gestión de la seguridad de la información permitirá proteger la

información generada y contenida en cualquier medio de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información académicos, financieros, de talento humano y tecnológicos, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de sus objetivos. Considerando que la información es un recurso muy importante y estratégico para cualquier organización ésta debe ser debidamente protegida.

TEORÍA Y CONTEXTO

Seguridad de la información

Actualmente para todas las organizaciones, la información es un instrumento fundamental para su funcionamiento, y el que necesita de una mayor protección ya que el uso intensivo del Internet y la tecnología ha originado que las amenazas que aprovechan las vulnerabilidades de las organizaciones hayan aumentado, ocasionando que se pierdan alguna de las características que la seguridad de la información debe preservar es decir la disponibilidad, la integridad y la confidencialidad de la misma (Areitio, 2008). Estas 3 características que contribuyen a lograr la seguridad de la información están estrechamente relacionadas entre sí, como puede observarse en la Figura 1.

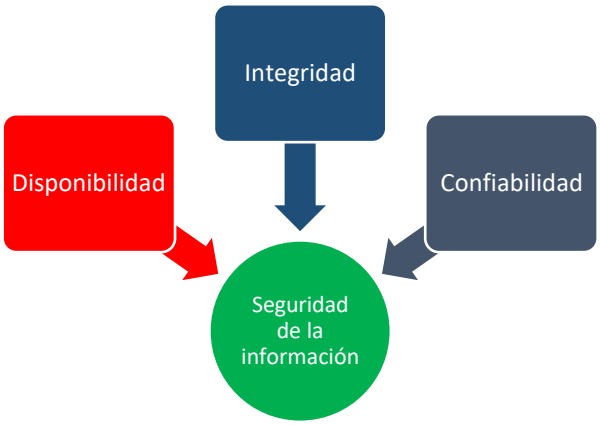


Figura 21. Características de Seguridad
Fuente: Adaptado de (Gómez Á. , 2014)

Las instituciones de educación superior como cualquier otra organización dependen también de la información para alcanzar sus objetivos estratégicos con calidad y excelencia, de manera que puedan cumplir con las expectativas tanto de sus clientes que serían los alumnos, como de proveedores y organismos de control del estado, especialmente en los procesos continuos de control y evaluación por parte de estos organismos.

De acuerdo con la norma ISO 27000 (2018), la información es considerada un activo, incluso mucho más significativo que otros por su importancia estratégica, por esta razón debe ser protegida de cualquier riesgo. La información no necesariamente está almacenada de forma digital, sino que en general se considera que puede estar también en forma física es decir impresa e inclusive el conocimiento que tienen las personas que realizan un trabajo específico.

Los elementos de la gestión de seguridad de la información entre otros incluyen: las políticas, normas, procedimientos, evaluación de los riesgos que puede sufrir la información y un tratamiento de

dichos riesgos mediante la implementación de controles de seguridad que permitan minimizarlos.

Sistema de Gestión de Seguridad de la Información (SGSI)

Uno de los métodos a disposición de las organizaciones para el manejo de la seguridad es el establecimiento de un Sistema de Gestión de Seguridad de la Información (SGSI), que de acuerdo con Giménez (2014), son las acciones o pasos que permiten establecer, implementar, mantener y mejorar continuamente la seguridad de la información, basándose en una determinación de los riesgos que se pueden presentar en la organización. Como expresa la norma ISO 27000 (2018), el SGSI es por lo tanto un proceso sistemático que necesita el apoyo de las autoridades y de toda la organización.

El SGSI debe determinar los diferentes riesgos a los que podría estar expuesta la información para determinar las políticas, procedimientos, controles o métodos para minimizar estos riesgos, todos esto procedimientos deben documentarse y socializarse; según Gómez y Fernández (2018), un SGSI se organiza en las cuatro fases típicas del ciclo Deming o ciclo de mejora continua, es decir: planear, hacer, verificar y actuar cuya relación se indica en la Figura 2.

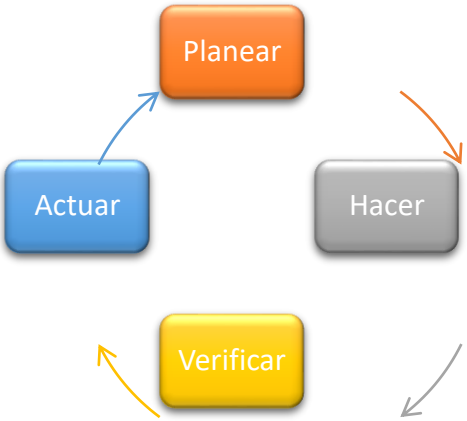


Figura 22. Ciclo de mejora continua
Fuente: adaptado de (Gómez & Fernández, 2018)

Estándares que rigen la Seguridad de la Información.

- ✓ **Norma BS7799-2**: proporciona un marco de referencia para establecer y administrar un Sistema de Gestión de Seguridad (SGSI). El propósito de la BS7799 es proteger la información de una amplia gama de amenazas garantizando la continuidad del negocio y minimizando los daños, da importancia a los procedimientos y mecanismos para mejorar la seguridad de la información. Sus objetivos son: proporcionar una guía de mejores prácticas de seguridad de la información, ayudar a la organización a identificar la fortaleza y la debilidad en los procesos de gestión de seguridad de la información y planear acciones de mejora que apoyen el logro de los objetivos de la organización (Haiwen & Graham, 2000).

- ✓ **O-ISM3:** Es una norma de madurez de la gestión de la seguridad de la información, publicado por The Open Group, define los define los procesos de seguridad para administrar un sistema de gestión de seguridad de la información (SGSI) en una organización, se debe definir los objetivos de seguridad requeridos en la Política de seguridad, ofrece un conjunto de procesos de administración de seguridad a partir de los cuales la organización selecciona cuáles implementar en el SGSI (Canal, 2017).

En esta norma, cada proceso de control de seguridad en el SGSI devuelve métricas para indicar de qué manera este proceso está contribuyendo al logro de los objetivos de seguridad. Esta retroalimentación de las métricas diferencia a esta norma de otras que definen también un SGSI.

- ✓ **Serie ISO/IEC 27000:** La serie de normas internacionales ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 emitidas por la Organización Internacional de Normalización (ISO) y la International Electronic (IEC) describe la manera en la que se debe gestionar la seguridad de la información en una organización, los conceptos relacionados con la seguridad y los sistemas de gestión, los requisitos de los SGSI, los controles de seguridad y la gestión de riesgos.
- ✓ **ISO/IEC 27001:2013**: Denominada por la ISO como "Tecnologías de la información - Técnicas de Seguridad - Sistemas de Gestión Seguridad de la Información – Requisitos". La revisión más reciente de esta norma fue publicada en el 2013, es la norma principal de la serie ISO/IEC 27000, su objetivo es establecer los requisitos para el diseño y la implementación de un SGSI de una forma bastante general de tal manera que sea aplicable a cualquier organización (ISO, Standart ISO/IEC 27001:2013, 2013).

Metodologías de la Gestión de Riesgos

Una de las actividades más importantes en el desarrollo de un SGSI es decidir la metodología de gestión de riesgos con la que se va a trabajar, ya que existen varias ya definidas que pueden utilizarse y que se alinean con la ISO/IEC 27001 (Vanegas & Pardo, 2014), o inclusive se puede adoptar una propia que cumpla con los requerimientos de la norma, sin embargo debe estar claramente establecida para poder repetirla, es decir que se pueda utilizar de la misma manera siempre, para que los resultados sean apropiados.

- ✓ **MAGERIT:** Utilizada por las empresas públicas españolas enfocado a la gestión de riesgos de la información. MAGERIT implementa la gestión de riesgos dentro de un marco de referencia que les permita a las organizaciones tomar decisiones a partir de

los riesgos encontrados en el uso de las TI (MHAP, 2012).

- ✓ **OCTAVE:** Desarrollada en el Centro de Coordinación CERT en *Carnegie Mellon University*. Octave es un método para la evaluación del riesgo. es una metodología para empresas grandes; Octave-S, similar a la original, pero para empresas mediana; y Octave Allegro, una metodología con un proceso simplificado con un uso más fácil (García, 2015).

- ✓ **RISK IT:** Publicado por ISACA, es un marco de referencia que se enfoca en las TIC, proporciona una visión global de los riesgos de la organización, es una herramienta práctica para la gestión de riesgos basada en el valor y beneficios que la organización obtiene a través de sus proyectos tecnológicos, se concentra en el cumplimiento de los objetivos de la organización. Este modelo puede utilizarse en cualquier tipo de empresa, y ofrece una serie de guías para la gestión eficaz de los riesgos (Vanegas & Pardo, 2014).

- ✓ **ISO/IEC 27005:** Es compatible con los requerimientos que establece la norma ISO/IEC 27001 en la sección 6. En la Figura 3 se indica los pasos establecidos para la gestionar los riesgos.

Figura 23. Ciclo de la gestión de riesgos

Fuente: (ISO/IEC, 20013)

II. METODOLOGÍA

El presente trabajo se basa en una metodología con las siguientes características:

- ✓ **Investigación descriptiva**: se ha realizado una descripción de la situación actual de la Universidad, se realizó un inventario de los activos de información, identificó los riesgos y determinó el tratamiento adecuado de estos, según los objetivos establecidos inicialmente

- ✓ **Enfoque cuantitativo**: se miden, comparan y describen las variables.

Población y muestra

Población: Este trabajo de investigación comprende la comunidad universitaria que está distribuida en tipos de población como se muestra en la Tabla 1.

Tabla 23. Población

Unidad administrativa	Personal
Directivos	17
Docentes	12
Administrativos	15
Total	**44**

Fuente: Elaborado por el autor

Muestra: La muestra se obtuvo a través de un muestreo intencional o de conveniencia, y fue de 27 personas, que corresponden a los responsables del manejo de activos de información en cada una de las direcciones, distribuidos de la manera que se indica en la Tabla 2.

Tabla 24. Distribución de la muestra

Área		**Empleados**
Dirección Académica	Directivos	7
	Docentes	12
	Administrativos	3
Dirección Financiera	Directivos	1
	Administrativos	2
Dirección de Talento Humano	Directivos	1
Dirección TIC	Directivos	1
Total		**27**

Fuente: Elaborado por el autor

Recolección de Información

Como técnicas de recolección de datos se utilizaron: encuestas, entrevistas, fichas de observación y evidencia documental.

- ✓ **Encuestas:** Se realizó una encuesta que se aplicó a la muestra seleccionada para determinar la cultura institucional sobre seguridad de la información, es decir el conocimiento que tienen sobre esta y la existencia de políticas, normas y procedimientos de seguridad de la información.

- ✓ **Entrevistas**: Se realizó entrevistas a personal de las direcciones Académica, Financiera, Talento Humano y TIC (Anexo 2), y se utilizó para realizar el inventario inicial de activos de información que consideran importante para sus funciones, para la valoración de dichos activos con un nivel de criticidad en el caso de que ocurra un evento de seguridad que afecte la disponibilidad, integridad o confidencialidad y el análisis de las amenazas y vulnerabilidades que pueden presentarse para cada activo.

- ✓ **Observación directa:** Para realizar la evaluación de riesgos, se utilizó la observación directa con una lista de chequeo donde se estableció los activos más importantes desde el punto de vista de los procesos de negocio, en el que se describe también el nivel de criticidad de cada activo, tomando como punto de partida las

entrevistas realizadas a las personas responsables de los procesos.

Situación actual

De los resultados obtenidos se puede evidenciar que la Universidad no cuenta en la actualidad con un sistema de gestión de la seguridad de la información (SGSI), ni con una política de Seguridad de la Información, los procedimientos de seguridad existentes son los que cada persona considera apropiadas para su trabajo; por tanto, es importante desarrollar el SGSI y un Plan Director de Seguridad a fin de mejorar la seguridad de la información en toda la organización y adaptarla al estándar ISO/IEC 27001.

Tampoco ha existido capacitación sobre la seguridad de la información ni sobre procedimientos, reglamentos o normas al respecto o cómo proceder en caso de que exista un incidente de seguridad que involucre activos de información.

Se ha logrado determinar las fortalezas y debilidades que pueden influir en la implantación de un Sistema de Seguridad de la Información y la situación inicial de la cultura de seguridad de la información en los empleados de la Institución.

Adicionalmente mediante la entrevista se pudo determinar un inventario preliminar de activos de información con detalles del medio en el que se encuentran (físico o digital), el tipo de información (interna, confidencial, externa) y el impacto de que se presente una amenaza sobre su disponibilidad, integridad y confidencialidad sobre dicha información.

III. PROPUESTA

Para el desarrollo del presente trabajo se seguirán siguieron los pasos que determinados por la norma ISO/IEC27001 para el desarrollo de un SGSI, adicionalmente se eligieron los controles de seguridad que la ISO/IEC27002 establece y que fueron adecuados para la Universidad, de acuerdo con el resultado que se determinó de la gestión de riesgos

Fase I Contexto de la organización

La Universidad es una institución de educación superior de carácter privado, con un tamaño pequeño, cuenta con alrededor de 45 empleados entre administrativos y docentes a tiempo completo, 64 docentes a tiempo parcial y un promedio de 600 alumnos. Tiene alrededor de 10 años de funcionamiento y cuenta con una sede única ubicada en la ciudad de Quito.

Actualmente la institución está trabajando en el establecimiento de un Sistema de Calidad bajo la norma ISO 9001, para lo que se encuentra definiendo sus procesos, debido se considera importante trabajar también en el diseño de un Sistema de Gestión de seguridad de la Información, que complemente el Sistema de Calidad.

Fase II Liderazgo

La segunda parte del SGSI en la norma ISO/IEC 27001 establece el liderazgo de la alta dirección, es decir las autoridades de la institución, que deben

manifestar su apoyo al proyecto con actividades como determinar los objetivos que se pretenden alcanzar con la implementación del SGSI, aprobar las Políticas Generales de Seguridad de la Información, definir los roles y responsabilidades del personal en relación con la seguridad de la información, entre otros.

Alcance

La cláusula 4.5 de la norma ISO 27001, establece que la organización determinará los límites o el alcance del sistema de gestión de la seguridad de la información. De acuerdo con esto, las autoridades han determinado el alcance del SGSI en la institución a los procesos: Gestión Académica, Financiera, Talento Humano y TIC, debido a que estos son los procesos que manejan la mayor parte de los sistemas de información de la institución, que determinan sus objetivos de negocio.

Objetivos del SGSI

Los objetivos de seguridad propuestos para el SGSI son los siguientes:

- ✓ Incrementar la seguridad de la información mediante la implementación de controles que permitan minimizar la pérdida de integridad, disponibilidad y confidencialidad de la información manejada en los procesos: Académico, Financiero, Talento Humano y Tecnologías de la Información y Comunicación.
- ✓ Mantener un registro y respuesta adecuada a incidentes y amenazas a la seguridad de la información.
- ✓ Mejorar la imagen frente a los clientes y entidades reguladoras al mejorar el manejo de la información en los procesos de la institución
- ✓ Optimizar el presupuesto destinado a las TIC con respecto a los proyectos de seguridad de la información.

Crear políticas de seguridad adecuadas para la institución, que deberá ser acatada por todos los trabajadores para mantener en todo momento la seguridad de la información.

Fase III Planificación: Gestión de riesgos de la información

En esta fase se realiza la gestión de riesgos, se define la metodología que se utilizará para este procedimiento, ésta incluye el inventario de los activos de información, la valoración de los activos, la detección de vulnerabilidades, amenazas y riesgos que pueden sufrir dichos activos en los procesos que están dentro del alcance del SGSI y el tratamiento de estos.

Para recolectar la información se aplicaron las técnicas de entrevistas a los usuarios de los sistemas y a los responsables de los procesos y la observación directa.

Inventario de activos de información

De acuerdo con el alcance definido para el SGSI se realizó un inventario de los activos de información en los procesos Académico, Financiero, Talento Humano y TIC, según la norma ISO/IEC 27005 los activos de información pueden ser: primarios y de soporte, en los primarios están las actividades y procesos y la información (documentos y datos) y en los de soporte están el hardware, software, redes, personas, sitios, organización.

El inventario de activos de información se realizó con los responsables de los procesos y usuarios que manejan información en las áreas que están dentro del alcance del SGSI.

Determinar amenazas y vulnerabilidades de los activos

Como otro paso se realizó el análisis de las amenazas y vulnerabilidades que pueden dar origen a los riesgos en los activos de información considerando la probabilidad de ocurrencia de un riesgo y el impacto que tendría sobre las 3 características de la seguridad de la información: disponibilidad, confidencialidad e integridad en los activos de información.

Para la evaluación de las amenazas y vulnerabilidades se parte de tablas de amenazas y vulnerabilidades conocidas, que están disponibles en diferentes fuentes, la norma ISO/IEC 27005. En la Tabla 3 se puede observar algunos ejemplos de amenazas.

Tabla 25. Ejemplos de Amenazas

Tipo	Amenaza
Deliberadas	Malware
	Denegación de Servicio
	Alteración de Información
	Destrucción de Información
	Fugas de Información
	Acceso no autorizado a la Información
	Suplantación de Identidad
	Abuso de privilegios de acceso
	Interceptación de información
	Manipulación de programas
	Ingeniería Social
	Manipulación de configuraciones
Naturales	Terremotos
	Erupción Volcánica
Accidentales	Corte de Suministro eléctrico
	Condiciones inadecuadas de temperatura o humedad
	Errores de mantenimiento/ actualización
	Agotamiento de recursos
	Indisponibilidad del personal
	Fallo de servicios de comunicaciones
	Interrupción de servicios de soporte
	Errores de usuarios
	Errores de administrador
	Errores de configuración
	Incendios

Fuente: (ISO/IEC, 2013)

Fase IV Documentación del SGSI

La Declaración de aplicabilidad muestra los controles de la norma ISO/IEC 27002 y del Anexo A de la ISO/IEC 27001 que son relevantes para el

SGSI de la Universidad y que permiten adicionalmente mitigar los riesgos encontrados en la etapa de análisis de riesgos, permite también verificar que se han considerado todos los controles previstos en la norma.

Fase V Plan de Implementación del SGSI

El plan de implementación del SGSI se presenta en la Tabla 4, este plan debe ser aprobado por las autoridades para comenzar con la implementación del proyecto.

Tabla 4. Plan de implementación del SGSI

Actividad	**Responsables**
Creación de plan de trabajo	Director TIC, autoridades
Definición del alcance del SGSI	Director TIC, autoridades
Definición de la política de seguridad	Director TIC, autoridades
Definición de roles y responsabilidades	Director TIC, autoridades
Identificación de los activos de información	Oficial de Seguridad
Definición del enfoque del análisis de riesgo	Comité de Seguridad de la información
Metodología de análisis de riesgo	Comité de Seguridad de la información
Tratamiento de los riesgos	Comité de Seguridad de la información
Selección de controles	Oficial de Seguridad
Declaración de aplicabilidad	Oficial de Seguridad
Planes de tratamiento de riesgo	Oficial de Seguridad
Implementación y puesta en marcha de proyectos	TIC, directores de área
Gestión de los recursos	Comité de Seguridad de la información
Formación y capacitación	Director de Talento Humano
Definir conjunto objetivos y métricas	Oficial de Seguridad
Evaluación del desempeño del SGSI	Auditor interno
Realizar auditorías internas	Auditor interno
Revisión por la dirección	Autoridades
Definir acciones correctivas	Comité de Seguridad de la información
Plan de mejora continua	Comité de Seguridad de la información, Oficial de Seguridad
Documentación del SGSI	Oficial de Seguridad

Fuente: Elaboración propia

CONCLUSIONES

Las normas internacionales de la familia ISO/IEC 2700 para la seguridad de la información dan un marco referencial para gestionar la seguridad en la institución, permitiendo de esta manera visibilizar el estado actual de la institución y planear estrategias de cambio y mejora continua en el manejo de la seguridad de la información, definiendo objetivos de seguridad que la Universidad puede alcanzar con un proceso sistemático y documentado.

De acuerdo con el levantamiento de información realizado en la situación actual de la Universidad se pudo determinar que actualmente en la institución no existe un Sistema de Gestión de Seguridad, no hay una cultura sobre seguridad de la información y no existen normas ni procedimientos

documentados ni aprobados que deban ser de cumplimiento obligatorio en las actividades normales de trabajo de la comunidad universitaria en relación con la seguridad de la información. Sin embargo, la Universidad está trabajando en la descripción y documentación de procesos con la implementación del sistema de calidad, esto hace que por un lado las persona que trabajan en la institución adquieran ya un conocimiento de la manera en que trabajar un sistema de gestión y por otro al definir sus procesos tengan ya una idea más clara de la información que manejan para realizar su trabajo.

El diseño de un Sistema de Seguridad de la Información para la universidad del caso de estudio, puede ser un gran paso para que la institución aumente su competitividad y mejore la calidad de sus procesos, ya que las organizaciones pequeñas pueden obtener grandes beneficios al tener un marco de referencia en los cuales organizar su planes y proyectos de una manera que se mitiguen los riesgos a los que podría estar expuesta con un desembolso de recursos acorde a su tamaño y necesidades, sin gastos que usualmente no sean necesarios para la Universidad. Además, al tener políticas, normas y procedimientos establecidos y conocidos, las personas que trabajan en la institución van a conocer cómo manejar los activos de información de forma que estén menos expuestos a riesgos de seguridad y si estos se presentan saber la manera en que deben proceder, para minimizarlos.

REFERENCIAS

Areitio, J. (2008). Seguridad de la información. Redes, informática y sistemas de información. Madrid: Paraninfo.

Canal, V. (30 de enero de 2017). About O-ISM3. Obtenido de https://www.ism3.com/node/42

Casillas, M. (13 de Junio de 2018). inbest.solutions. Obtenido de https://inbest.solutions/que-es-un-drp/

García, Y. (2015). Modelo de gestión de la seguridad de información en los procesos críticos de las áreas financieras universitarias. Caso PUCE. Quito.

Gómez , L., & Fernández, P. (2018). Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad. Madrid: AENOR.

Gómez, Á. (2014). Seguridad en equipos informáticos. Madrid: RA-MA.

Haiwen, L., & Graham, K. (2000). BS7799: A Suitable Model for Information Security Management. AMCIS 2000 PROCEEDINGS.

ISO. (2013). Standart ISO/IEC 27001:2013. Information technology - Security techniques. ISO.

MHAP. (2012). MAGERIT. Metodología de

Análisis y Gestión de Riesgos de los Sistemas de Información. Obtenido de https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Vanegas, G., & Pardo, C. (2014). Hacia un modelo para la gestión de riesgos de TI en MiPyMEs: MOGRIT. Sistemas & Telemática, 12(50), 48 - 55.