UNIVERSIDAD INTERNACIONAL DEL ECUADOR

Facultad de Ciencias Administrativas y Económicas

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE MAGÍSTER EN ADMINISTRACIÓN DE EMPRESAS

MODELO DE GESTIÓN TECNOLÓGICA QUE GARANTICE LA FIABILIDAD Y SEGURIDAD DE REPOSITORIOS DIGITALES DE INFORMACIÓN DE INSTITUCIONES DE EDUCACIÓN SUPERIOR

AUTOR: EDGAR RAMIRO SÁNCHEZ MEZA

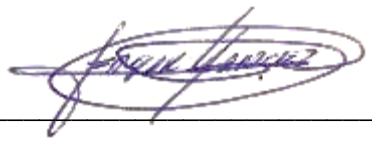
DIRECTOR: CHRISTIAN PAÚL BERNIS LLANOS

2021

Quito-Ecuador

Yo, Edgar Ramiro Sánchez Meza, declaro que soy el autor exclusivo de la presente investigación; y que ésta es original, auténtica y personal. Para todos los efectos académicos y legales que se desprendan de la presente investigación serán de mí sola y exclusiva responsabilidad.

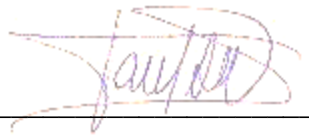
Cedo mis derechos de propiedad intelectual a la UIDE, según lo establecido en la Ley de Propiedad Intelectual, reglamento y leyes.



_____

Edgar Ramiro Sánchez Meza

Yo, CHRISTIAN PAÚL BERNIS, Declaro que, en lo que yo personalmente conozco, el graduado Edgar Ramiro Sánchez Meza es el autor exclusivo de la presente investigación y que ésta es original, autentica y personal.



_____

Christian Paúl Bernis Llanos

AGRADECIMIENTOS

A la Universidad Internacional del Ecuador, a todos sus profesores y personal administrativo por su apoyo durante el tiempo transcurrido en la maestría.

Agradezco también a todos los compañeros de la Promoción XIII, con los cuales pude compartir esta nueva experiencia estudiantil. Para todos ellos, muchos éxitos en su vida profesional.

Edgar

DEDICATORIA

A quién me acompañó durante mucho tiempo, me vio crecer, disfrutó de mi éxito y fue mi consuelo en mis fracasos, quien me animó en todo momento y siempre tenía una palabra de aliento, para el señor San está dedicado este trabajo.

Edgar

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

Las instituciones de educación superior en Ecuador constituyen los centros educativos que imparten carreras de nivel superior de tercer y cuarto nivel. La oferta académica es variada en carreras técnicas y administrativas. Dentro de las funciones principales son la docencia, "generación y aplicación innovadora del conocimiento, así como la extensión y difusión de la cultura" (Secretaría de Educación Pública [SEP], s.f., párr. 3).

La Constitución de la República del Ecuador establece que el Sistema de Educación Superior se regirá por un organismo público de planificación, regulación y coordinación interna del sistema, adicionalmente, de la relación entre sus distintos actores con la Función Ejecutiva, en conjunto con un organismo público técnico de acreditación y aseguramiento de la calidad de instituciones, así como de las carreras y programas dentro de las mismas. (Asamblea Nacional Constituyente de Ecuador, 2008, art. 353)

Con relación a la problemática expuesta y para cumplir con el estándar requerido por el organismo de control, en el que se solicita una plataforma informática disponible y accesible a la comunidad universitaria para la gestión de los procesos académicos y administrativos, el presente trabajo propone un modelo de gestión de tecnologías de información, en cuyo caso se convierte en una herramienta de gestión administrativa, con la cual, las áreas directiva y técnica de la institución puedan cumplir la misma visión del cumplimiento normativo.

Palabras clave: educación superior, gestión, información, acreditación, cumplimiento.

ABSTRACT

The Higher Education Institutions in Ecuador constitute the educational centers that teach third and fourth level higher level careers. The academic offer is varied in technical and administrative careers. The main functions are the teaching, generation, and innovative application of knowledge, as well as the extension and diffusion of culture.

The Constitution of the Republic of Ecuador establishes that the Higher Education System will be governed by a public body for planning, regulation and internal coordination of the system and the relationship between its different actors with the Executive Function, and by a technical public body for accreditation and quality assurance of institutions, careers, and programs.

In relation to the exposed problem, to comply with the standard required by the control body, which requests a computer platform available and accessible to the university community for the management of academic and administrative processes; This work proposes an information technology management model, which becomes an administrative management tool, with which the directive area and the technical area of the institution can fulfill the same vision of regulatory compliance.

Keywords: Higher Education, Management, Information, Accreditation, Compliance.

Capítulo I. Introducción

1.1 Problema de investigación

Las Instituciones de Educación Superior (IES) están supervisadas por organismos de control gubernamental. Estas instituciones se encargan de hacer cumplir los hitos considerados en su normativa, garantizando que las Universidades y Escuelas Politécnicas proporcionen educación de calidad a sus estudiantes.

Una de las condiciones necesarias para el cumplimiento de los requisitos solicitados por el organismo de control está relacionado con la infraestructura y el equipamiento tecnológico, donde se contemplan diferentes variables como, por ejemplo: políticas, estándares, gobierno de tecnología, continuidad de negocio, infraestructura tecnológica.

Al existir dicha normativa y a causa de sus dimensiones de cumplimiento, se entiende que no todas las Instituciones de Educación Superior están en la capacidad de alinear los requerimientos solicitados y presentarlos en forma organizada de tal forma que, sean un valor agregado a la planificación estratégica institucional.

1.2 Tema del trabajo de investigación

Modelo de gestión de tecnologías de información para garantizar la fiabilidad y seguridad de los repositorios de información para instituciones de Educación Superior en Ecuador.

1.3 Objetivos de la investigación

1.3.1 Objetivo general

Proponer un modelo de gestión tecnológica que garantice la fiabilidad y seguridad de los repositorios digitales de información de Instituciones de Educación Superior en el Ecuador.

1.3.2 Objetivos específicos

1) Analizar los requerimientos base solicitados por los organismos de control con respecto a la organización del área tecnológica de las Instituciones de Educación Superior.
2) Definir el modelo de gestión de seguridad adecuado, mediante la adaptación de metodologías, marcos de trabajo o buenas prácticas que describan la gestión de seguridad en las tecnologías de la información.
3) Establecer el marco de trabajo que sirva como modelo referencial para la gestión de seguridad de tecnologías de la información en las áreas tecnológica y administrativa de una Institución de Educación Superior.
4) Proponer un modelo de gestión de tecnologías de la información, el cual garantizará la seguridad de los datos almacenados en los repositorios institucionales.

1.4 Justificación práctica y delimitación de la investigación

El entorno de la información que se genera en una institución involucra varios aspectos que afectan los diferentes procesos de negocio, por consiguiente surge la necesidad de mejorar, controlar, agilizar y asegurar todos los procesos que involucren la gestión de datos y por lo tanto la seguridad de la información; como consecuencia se genera una inquietud acerca de la

implementación de un modelo de gestión de tecnologías de la información aplicando la guía de buenas prácticas para la Gestión de Servicios de tecnologías de información.

Con la finalidad de establecer un adecuado gobierno corporativo, el marco de trabajo denominado COBIT, ayuda a controlar y evaluar los procesos, mientras que a su vez mantiene la seguridad de los sistemas informáticos.

Resulta claro que en la actualidad las Tecnologías de la Información y Comunicaciones (TIC), han crecido con una rapidez exponencial y se encuentran presentes no solo en pequeñas organizaciones sino también se las implementa en multinacionales, por tal motivo las TICs, se han involucrado en las organizaciones tanto en el área administrativa como en el área operativa con la finalidad de proveer de seguridad a las mismas.

Uno de los campos de la Tecnología de la Información es el encargado de proteger activos digitales dentro de la organización, tales como información confidencial, accesos a sus computadores de trabajo, archivos de clientes y otros elementos propios de las organizaciones. Es por esta razón y a causa de dicha necesidad que se han creado metodologías, herramientas y técnicas que son de utilidad para poder asegurar o salvaguardar la información o los datos importantes de las organizaciones; este es uno de los puntos que se puede evaluar al realizar un estudio relacionado con la seguridad de datos, su entorno y la gestión necesaria para la organización de los datos dentro una institución de forma segura.

Con el nacimiento de la Seguridad Informática se da cumplimiento a los objetivos enfocados en salvaguardar la información en tres aspectos fundamentales: integridad, disponibilidad y confidencialidad, finalmente se debe tener en cuenta que la seguridad de la

información “debe hacer frente a los riesgos, analizarlos, prevenirlos y encontrar soluciones rápidas para eliminarlos” (Tecon, s.f., párr. 2).

Para el presente trabajo se ha tomado en cuenta el documento emitido por el ministro de Telecomunicaciones de Ecuador, Andrés Michelena, quien fue el encargado de su entregar el proyecto de Ley de Protección de Datos Personales a la Asamblea Nacional “el jueves 19 de septiembre del 2019, días después de que se conociera la filtración masiva de datos de ecuatorianos.” (Agencia EFE, 2019, párr. 1)

El Ministerio de Telecomunicaciones tiene “una propuesta que se enmarca en una estrategia más amplia denominada Ecuador Digital” (Pichincha Comunicaciones, 2019, párr. 3), la cual pretende “digitalizar el Gobierno y todos los sectores del país” (párr. 3). Bajo este orden de ideas, el primer paso será constituir un marco regulatorio estructural, el cual se fundamenta en la capacidad de tener una protección de los datos personales, para que los ciudadanos en el marco de sus derechos y garantías puedan escoger qué información es pública y cómo se utiliza, en este contexto, es prioridad que las Instituciones de Educación Superior proporcionen servicios seguros que garanticen la seguridad, confidencialidad y disponibilidad de la información de los estudiantes, docentes y colaboradores administrativos.

1.5 Tipo de investigación

La investigación de este estudio está basada en los documentos normativos a cumplir por las Instituciones de Educación Superior y las variables inmersas en el mismo. Por lo tanto, es un tipo de investigación transversal.

1.6 Población y muestra

"La población del objeto de estudio está constituida" (Ortega & Calderón-Salazar, 2014, p. 93) por las Instituciones de Educación Superior del Ecuador.

1.7 Fuentes de recolección de información

Las fuentes de recolección de información secundaria comprenden los modelos de evaluación, las normativas, metodologías, marcos de trabajo e informes.

1.8 Técnicas de recolección de información

La técnica de recolección de información consistió en el análisis de los siguientes documentos:

- Modelo de Evaluación Institucional de Universidades y Escuelas Politécnicas.
- Ley Orgánica de Educación Superior.
- Reglamento General a la Ley Orgánica de Educación Superior.
- Plan Nacional de Desarrollo, Plan Nacional para el Buen Vivir 2013-2017.
- Estrategia Nacional de Educación Ambiental para El Desarrollo Sostenible 2017-2030.
- Mejores prácticas.
- Metodologías.
- Marcos de trabajo.
- Análisis documental.

Capítulo II. Marco Teórico

Para el desarrollo de esta investigación es necesario conocer los principales conceptos que involucran el diseño de un modelo de gestión de tecnologías, que garanticen la fiabilidad y seguridad de repositorios digitales de información en las instituciones de educación superior.

2.1 Ley Orgánica de Educación Superior

La función de la Ley Orgánica de Educación Superior (LOES), consiste en regular:

> El sistema de educación superior, los organismos e instituciones que lo integran y determinar los derechos, deberes y obligaciones de las personas naturales y jurídicas, estableciendo las respectivas sanciones a causa del incumplimiento de las disposiciones contenidas en la Constitución y en la presente Ley.
>
> La LOES tiene como objetivo definir sus principios, garantizar el derecho a la educación superior de calidad que tiende a la excelencia, el acceso universal, permanencia, movilidad y egreso sin discriminación de ningún tipo. (art. 1)

2.2 Modelo de evaluación externa y acreditación de universidades y escuelas politécnicas

El Pleno del Consejo de Aseguramiento de la Calidad de la Educación Superior (CACES), aprobó el 14 de junio del 2019, democráticamente, “el Modelo de Evaluación Externa de Universidades y Escuelas Politécnicas” (Caces, s.f., párr. 1), cuyo contenido fue puesto en conocimiento de las instituciones de educación superior ecuatorianas, el estado y la ciudadanía,

así como de importantes redes de aseguramiento de la calidad de la educación superior internacional y de las diversas agencias extranjeras dedicadas a la importante tarea de la evaluación y acreditación educativa (Caces, 2019).

El modelo de evaluación del CACES fue elaborado gracias al aporte de las diferentes universidades, "está basado en tres ejes principales los cuales corresponde a las denominadas funciones sustantivas que involucran: la docencia, la investigación y la vinculación con la sociedad, en conjunto con el eje de condiciones institucionales" (Caces, 2019, p. 8). Las funciones sustantivas están organizadas con relación a su planificación, ejecución y resultados alcanzados por las instituciones a lo largo del tiempo. Para alcanzar el conocimiento del estado de una universidad o escuela politécnica el modelo analiza a cada institución a través de los 20 estándares definidos en su modelo de evaluación, como se puede observar en la figura 1, en el que se representan las condiciones esenciales con las cuales una institución puede ser parte del sistema de educación superior.

Figura 1. Ejes, dimensiones y número de estándares del modelo de evaluación.

Ejes de la evaluación	Dimensiones de la evaluación			Total de estándares
	Planificación	Ejecución	Resultados	
Función sustantiva Docencia (Profesorado y estudiantado)	2	2	3	7
Función sustantiva Investigación	1	1	2	4
Función sustantiva Vinculación con la Sociedad	1	1	1	3
Condiciones institucionales				6
				20

Fuente: elaboración propia

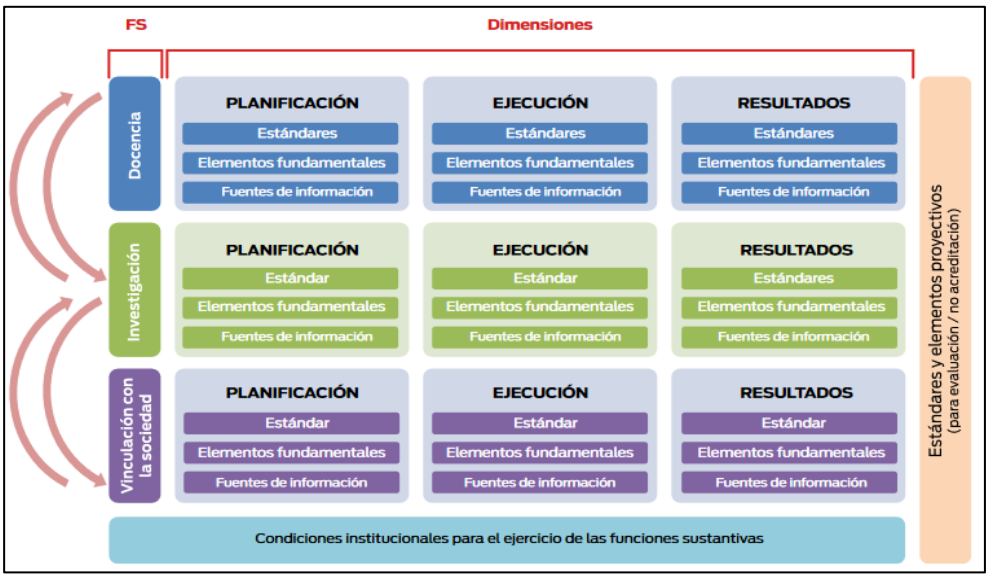
Para el desarrollo de las funciones sustantivas es necesario que las instituciones cumplan con varias "condiciones institucionales", como por ejemplo los procesos de planificación

estratégica y operativa, la infraestructura y los equipos informáticos, las bibliotecas, y la gestión interna del aseguramiento de la calidad.

> En cada una de las dimensiones se definen estándares que expresan la meta deseable que se pretende ser conseguida por las IES, y sobre la cual se evaluará a cada institución. Los estándares son de carácter cualitativo y cuantitativo, descomponiéndose los primeros en un conjunto de elementos fundamentales y los segundos en fórmulas de cálculo matemático. (Consejo de Aseguramiento por la Calidad de la Educación Superior, 2019, p. 23)

El esquema general de la estructura del modelo 2019 se lo puede analizar en la figura 2.

Figura 2. Esquema de la estructura del modelo 2019



Fuente: (Caces, 2019)

2.3 Función sustantiva – vinculación con la sociedad

En la tabla 1 se muestran los elementos fundamentales que se integran en la definición del modelo de gestión tecnológica que garanticen la fiabilidad y seguridad de los repositorios digitales de información de instituciones de educación superior.

Tabla 1. *Condiciones Institucionales.*

Estándar	Principio	Elementos fundamentales
15 Planificación Estratégica y Operativa	La institución cuenta con planificación estratégica y operativa institucional pertinente que orienta la gestión de las funciones sustantivas y las actividades institucionales; es ejecutada, monitoreada, evaluada y difundida por las instancias responsables, en coherencia con su modelo educativo y con la debida participación de la comunidad universitaria.	15.1. La institución aplica normativa y/o procedimientos, aprobados y vigentes, para planificar sus estrategias de desarrollo institucional, alineadas con su modelo educativo, bajo el principio de pertinencia. 15.3. La planificación estratégica institucional establece directrices para el desarrollo y el mejoramiento continuo de las funciones sustantivas y de las actividades institucionales; la planificación operativa anual prevé los recursos financieros y humanos necesarios para dar cumplimiento a lo programado.
16 Infraestructura y equipo informático	La institución cuenta con infraestructura y equipamiento físico e informático funcional y suficiente, para el desarrollo de las actividades académicas y administrativas, atendiendo a las necesidades de personas con discapacidad bajo la gestión de instancias responsables.	16.5 La institución cuenta con una plataforma informática disponible y accesible a la comunidad universitaria para la gestión de los procesos académicos y administrativos.

Fuente: adaptado de Modelo de evaluación externa de universidades y escuelas politécnicas.

2.4 Gobierno corporativo

Mediante Resolución No. SCVS-INC-DNCDN-2020-0013, suscrita el 1 de septiembre del 2020, la Superintendencia de Compañías, Seguros y Valores aprobaron las Normas ecuatorianas para el Buen Gobierno Corporativo. La implementación del gobierno corporativo en el sector empresarial es una herramienta vital para la investigación desarrollada, de tal manera que este sistema de organización y gestión es el encargado de promover la transparencia en la información. Además, fortalece las relaciones del nivel directivo empresarial y proporciona respuestas sólidas ante situaciones de contingencia.

> El Gobierno Corporativo es el sistema de control y dirección de las sociedades mercantiles. Sucede pues, que abarca el conjunto de principios y normas que establecen los estándares elementales para (i) proteger los derechos de los socios o accionistas y la existencia de un trato equitativo entre ellos; (ii) establecer una administración transparente y responsable; (iii) dar fluidez a la información de la sociedad y recomendar mecanismos de control; (iv) regular las relaciones con los grupos de interés; (v) transparentar la información que se deriva de su operación; y (vi) establecer recomendaciones para que el ejercicio de las actividades de la compañía se lleve a cabo de una manera correcta, de acuerdo con los estándares éticos. (Resolución No. SCVS-INC-DNCDN-2020-0013, 2013, p. 1)

2.5 Planificación estratégica

La planificación estratégica es un proceso que requiere integrar los planes y programas de acción, los presupuestos, los sistemas de información y control; a su vez, esta indica las

acciones a emprender para conseguir los fines pertinentes, teniendo en cuenta la posición competitiva relativa, además de las previsiones e hipótesis sobre el futuro.

Los programas y planes de acción señalan qué se debe hacer, para quién, cuándo y con qué recursos. Los sistemas de información constituyen la base del control de cumplimiento del plan (Romero, 2004).

2.6 Marco de gobierno de tecnologías de información

Para la gobernanza, la gestión de la información para la tecnología institucional se incluye el marco de trabajo denominado COBIT. En el cual se incluye toda la tecnología y el procesamiento de información que la empresa apuesta en búsqueda de la consecución de sus objetivos, independientemente del área de la empresa. Es decir, la información y la tecnología no se limita exclusivamente al departamento de tecnologías de información (TI), de una organización, pero ciertamente, lo incluye. “El marco de COBIT hace una clara distinción entre gobernanza y gestión. Estas dos disciplinas abarcan diferentes actividades que requieren diferentes estructuras organizativas, las cuales sirven para diferentes propósitos” (Interpolados, 2016, párr. 5). De ahí que la gobernanza asegura que:

- “Las necesidades, condiciones y opciones de las partes interesadas” (Hernández, s.f., p. 6).se evalúen para determinar una empresa y acuerdos de los objetivos planteados.
- “La dirección se establece mediante la priorización y toma de decisiones” (p. 2).

- El desempeño y el cumplimiento se controlan en función de la dirección y los objetivos acordados.

En la mayoría de las empresas la gobernanza es responsabilidad del consejo de administración bajo el liderazgo del presidente de la empresa. Las responsabilidades específicas de gobernanza pueden delegarse a estructuras organizativas especiales en un nivel apropiado, particularmente en instituciones grandes o complejas. En este contexto, la gestión planifica, construye, ejecuta y supervisa las actividades en consonancia "con la dirección establecida por el gobierno para lograr los objetivos empresariales" (Salah, 2017, p. 86; Systems Audit and Control Association [ISACA], 2020).

2.7 Seguridad de la información

Constituye la disciplina empresarial que protege la información de su divulgación a usuarios no autorizados (garantizando la confidencialidad), su modificación indebida (garantizando la integridad), e impidiendo el acceso cuando sea necesario (garantizando la disponibilidad).

2.8 Indicador

Es un valor que establece una relación "entre dos o más datos significativos, de dominios semejantes o diversos y que proporciona información sobre el estado en que se encuentra un sistema" (Lugo, 2015, párr. 54).

2.9 Gobierno

Marco y sistema que garantiza que se evalúen “las opciones, condiciones y necesidades de las partes interesadas para determinar” (Rivadeneira y Pinedo, 2018, p. 27) unos objetivos empresariales equilibrados y acordados; por otro lado, garantiza que se establezca la dirección estratégica, se prioricen y respalden las metas mediante la toma de decisiones adecuadas y oportunas.

2.10 Riesgo

La combinación de la probabilidad de un evento y su impacto.

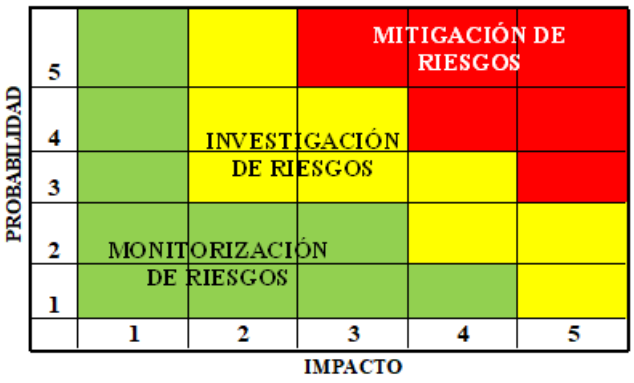
2.11 Matriz de riesgo

Una matriz de riesgos es también conocida como “Matriz de Probabilidad de Impacto”, de manera general, el riesgo se define como la probabilidad de que ocurra un evento no deseado, mismo que al materializarse puede generar pérdidas. La gestión de riesgos tiene como finalidad minimizar la posibilidad de ocurrencia del evento desfavorable a través de la identificación, medición, tratamiento, monitoreo y control de los riesgos, la cual es aplicada a los diferentes tipos de riesgos, tales como financieros, operativos, tecnológicos, etc.

Debido a que los riesgos pueden ser de varios tipos y diferente magnitud, es necesario tratarlos y gestionarlos de un modo sistemático enfocándose en los riesgos de nivel alto, lo que permitirá dimensionar el uso de los recursos disponibles. Así mismo, se puede construir una matriz de riesgos en la que se represente la probabilidad de ocurrencia de los peligros frente a la gravedad o severidad de sus consecuencias (impacto). La combinación de la probabilidad e

impacto determina el nivel de riesgo de un evento, el cual se puede observar en la figura 3, donde los riesgos se clasifican según su probabilidad muy baja 1, baja 2, media 3, alta 4 o muy alta 5, o también puede clasificarse en baja 1, media 2 y alta 3.

Figura 3. Matriz de riesgos



Fuente: elaboración propia

2.12 Ciberseguridad

La disciplina empresarial que protege los activos informáticos al abordar las amenazas a la "información procesada, almacenada y transportada por sistemas de información interconectados a través de redes" (SGSI, 2017, párr. 5).

2.13 Ciber riesgo

La exposición al peligro, daño o las pérdidas relacionadas con el uso o la dependencia de las tecnologías de la información y las comunicaciones, los datos electrónicos, y las comunicaciones digitales o electrónicas. Generalmente, la materialización del ciber riesgo

implica el acceso y/o uso no autorizado de las tecnologías de la información y las comunicaciones.

2.14 Cumplimiento normativo

> Es un conjunto de procedimientos y buenas prácticas adoptados por las organizaciones para identificar y clasificar los riesgos operativos y legales a los que se enfrentan, para lograr establecer mecanismos internos de prevención, gestión, control y reacción frente a los mismos. (World Compliance Association, 2021, párr. 1)

2.15 Committee Of Sponsoring Organizations of the Tradeway Commission

> Committee of Sponsoring Organizations of the Tradeway Commission (COSO), es una comisión voluntaria constituida por representantes de cinco organizaciones del sector privado de los Estados Unidos de América, para proporcionar liderazgo intelectual frente a tres temas interrelacionados entre sí, los cuales hacen parte de la gestión del riesgo empresarial, el control interno y la disuasión del fraude. (AEC, s.f., párr. 1)

COSO establece las "principales directivas para la implantación, gestión y control de un sistema de Control Interno y administración de riesgos" (Salvador, 2016, párr. 1). La arquitectura de control abarca los componentes: ambiente de control, gestión de riesgos, actividades de control, información, comunicación y monitoreo.

Capítulo III. Análisis del entorno

3.1 Análisis PESTEL

El análisis PESTEL es una herramienta de planeación estratégica que sirve para identificar el entorno sobre el cual se diseñará el proyecto de una forma ordenada y esquemática (Pérez, 2018; UDG virtual, s.f., p. 2). Este análisis estratégico determinará la situación de la IES, con la finalidad de crear estrategias, aprovechar oportunidades o actuar de manera eficaz ante posibles riesgos (Parada, 2013).

3.1.1 Factores Políticos

> El Artículo 351 de la Constitución de la República del Ecuador establece que el Sistema de Educación Superior estará articulado al sistema nacional de educación y al Plan Nacional de Desarrollo; la ley establecerá los mecanismos de coordinación del Sistema de Educación Superior en conjunto con la Función Ejecutiva. Este sistema se regirá por los principios de autonomía responsable, cogobierno, igualdad de oportunidades, calidad, pertinencia, integralidad, autodeterminación para la producción del pensamiento y conocimiento, dentro del marco del diálogo de saberes, pensamiento universal y producción científica tecnológica global. (Ley Orgánica de Educación Superior, 2018, art. 351)

Regula el sistema de educación superior en el país, a los organismos e instituciones que lo integran; determina derechos, deberes y obligaciones de las personas naturales y

> jurídicas, y establece las respectivas sanciones por el incumplimiento de las disposiciones contenidas en la Constitución y en la presente ley. (Ley Orgánica de Educación Superior, 2018, p. 1)

Mediante las reformas incorporadas a la LOES (Art. 171), publicada en el Registro Oficial Suplemento 297 del 2 de agosto del 2018, el Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad -CEAACES- cambia de nombre a el Consejo de Aseguramiento de la Calidad de la Educación Superior -CACES.

El Pleno del Consejo de Aseguramiento de la Calidad de la Educación Superior, el 14 de junio del 2019, aprobó el Modelo de Evaluación Externa de Universidades y Escuelas Politécnicas.

3.1.2 Factores Económicos

La crisis económica provocada a causa de la emergencia sanitaria decretada en el año 2020 provocó un corte en las reasignaciones del Gobierno del Ecuador a las universidades públicas, privadas y de posgrado, motivo por el cual se ha visto afectado el sector educativo.

> [De acuerdo con la previsión] del Banco Central del Ecuador para 2021 se estima que la economía se recupere y crezca un 3,1 %, equivalente a un Producto Interno Bruto (PIB) de USD 67.539 millones en valores constantes (figura 4). Esta recuperación en la economía ecuatoriana será dinamizada principalmente por el gasto de los hogares, en cuyo caso se incrementaría en USD 3.441 millones, gracias a mayores importaciones de

bienes de consumo (USD 136,2 millones), y un incremento en las remesas recibidas (USD 272,5 millones). (Angulo, 2020, párr. 8)

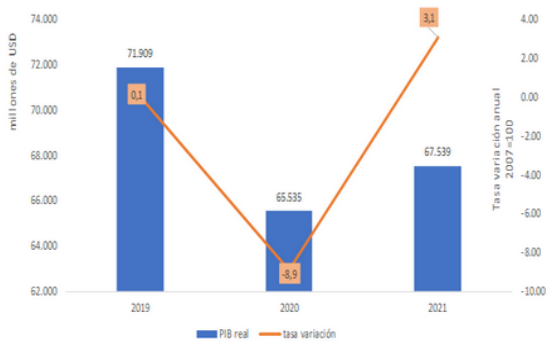
Figura 4. Previsión 2021

Tabla 1: Cuadro Oferta – Utilización
Tasas de variación 2007=100

Variables \ Escenarios	2019 prelim¹	2020 (prev)*	2021 (prev)*
Años	**2019**	**2020**	**2021**
P I B (pc)	0,1	-8,9	3,1
Importaciones	1,6	-10,5	3,2
OFERTA FINAL	0,4	-9,2	3,1
CONSUMO FINAL TOTAL	0,7	-7,4	3,1
Administraciones públicas	-2,5	-3,3	-1,3
Hogares	1,5	-8,5	4,2
Formación Bruta de Capital Fijo	-3,4	-19,4	-0,2
Exportaciones	5,2	-5,1	3,1
DEMANDA FINAL	0,4	-9,2	3,1

(prev)* corresponde a la previsión del año.
(prelim) corresponde a la sumatoria de trimestres de las Cuentas Nacionales Trimestrales.

Gráfico 1: PRODUCTO INTERNO BRUTO (PIB)
2007=100



Fuente: (Banco Central del Ecuador, 2020)

3.1.3 Factores Socioculturales

La Educación es la herramienta que permite a cualquier estado mejorar la calidad de vida de la población. Ecuador tiene definido en el Plan Nacional para el buen Vivir, en su objetivo 4, fortalecer las capacidades y potencialidades de la ciudadanía, esto guarda relación directa con la Política 4.2 la cual dictamina "Promover la culminación de los estudios en todos los niveles", es por esto que surge la importancia de que todo ciudadano se encuentre involucrado en el tema educativo. La importancia de que un estado apueste a un eje tan importante como lo es el educativo, genera una relación directamente proporcional hacia un país con un mejor futuro, gracias a que es un crecimiento proyectado a mediano y largo plazo en aras de generar una sociedad más culta y que esté en capacidad de elegir de la mejor manera el futuro de la patria. El país al contar con una educación inclusiva logra llegar a personas de diferente nivel socio

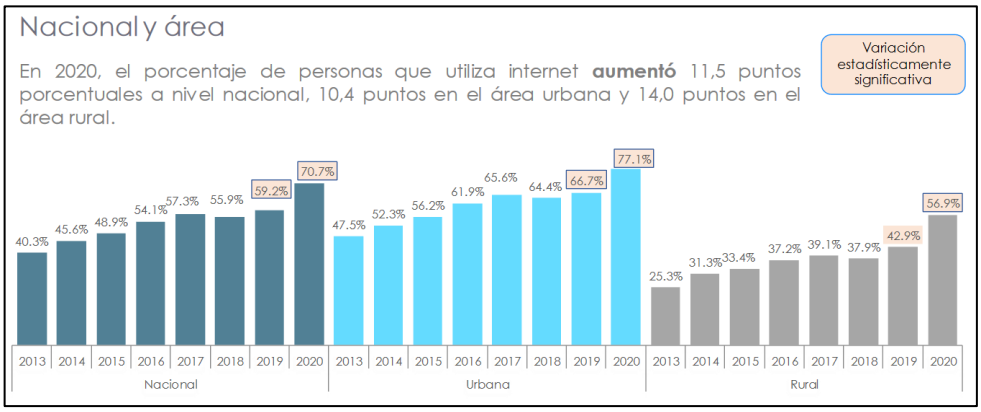
cultural, quienes tendrán en sus manos la responsabilidad de convertirse en un aporte positivo para la sociedad.

3.1.4 Factores tecnológicos

"Las TICs son todos aquellos recursos, herramientas y programas que se utilizan para procesar, administrar y compartir la información mediante diversos soportes tecnológicos" (Instituto Provincial de Administración Pública de Mendoza, s.f., p. 1), como consecuencia de este uso, todo dispositivo conectado a internet genera datos informáticos a partir de los cuales se contribuye a la formulación de políticas públicas y toma de decisiones por parte de las autoridades. El Instituto Nacional de Estadística y Censos (INEC), en su portal https://www.ecuadorencifras.gob.ec/ presenta el porcentaje de personas que utilizan internet. En la figura 5, se puede observar el incremento en el uso informático de los últimos años.

Según el estudio publicado en el portal INEC, las personas que han utilizado el servicio de internet desde cualquier lugar en los últimos 12 meses, corresponde a la población mayor a cinco años de edad (INEC, 2021).

Figura 5. Porcentaje de personas que utilizan internet



Fuente: (INEC 2021)

3.1.1 Factores Ecológicos

Ecuador cuenta con la Estrategia Nacional de Educación Ambiental para el Desarrollo Sostenible 2017 – 2030, creada por el Ministerio de Ambiente en el año 2017. Dentro de los ámbitos de acción definidos para la Estrategia Nacional de Educación Ambiental se encuentran: formal, no formal e informal. De modo que se ha identificado el sistema educativo como un eje que facilitará el desarrollo de la estrategia de manera articulada y participativa. Con este antecedente se ha incluido la Educación Superior organizada por instituciones de educación superior e institutos tecnológicos a la política pública establecida por la Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación.

Las instituciones de educación superior también pueden alinearse con los Objetivos de Desarrollo Sostenible de las Naciones Unidas, específicamente, con el objetivo de desarrollo sostenible número nueve cuya meta consiste en "la infraestructura básica, como las carreteras, las tecnologías de la información y la comunicación, el saneamiento, la energía eléctrica y el agua, sigue siendo escasa en muchos países en desarrollo" (Naciones Unidas, 2018, párr. 11).

3.1.2 Factores Legales

Dentro de los factores legales que afectan a la educación superior se consideran los largos procesos de aprobación de proyectos de inversión al sector de la educación superior pública, esto añadido al ineficiente cumplimiento de las leyes, lo cual produce un impacto jurídico – legal en la enseñanza superior. En el sector privado también se produce el mismo fenómeno debido a los amplios tiempos que generan en los procesos realizados por un ente burocrático para la gestión de los requerimientos de una IES.

Del análisis realizado, en la tabla 1 Condiciones institucionales, se pueden observar los riesgos encontrados y las oportunidades de mejora que estarán orientadas al modelo de gestión tecnológica, los cuales que garantizarán la fiabilidad y seguridad de repositorios digitales de información. A continuación, en la tabla 2 se presenta el análisis PESTEL, tomando en cuenta el estándar de infraestructura y equipo informático.

Tabla 2. *Análisis PESTEL*

Factores	Riesgos	Oportunidades
Políticos	Disminución de calidad en las instalaciones.	Incrementar las carreras universitarias con formación en línea. Establecer nuevas estrategias para enseñanza en plataformas de educación virtual.
Económicos	Incremento en los gastos realizados en casa, relacionados con herramientas educativas.	Promover programas de educación financiera.
Sociales	Deserción estudiantil debido al tipo de carreras que decidan los estudiantes.	Implementar herramientas telemáticas que permitan que los programas puedan ser impartidos a sus estudiantes.
Tecnológicos	Pérdida de información.	Concientización en las IES, para el buen uso de recursos tecnológicos.
Ecológicos	Problemas de salud debido al confinamiento.	Mediante herramientas informáticas apoyar a los integrantes de la IES en el aspecto emocional y psicológico.
Legales	Proyectos de infraestructura detenidos.	Actualizar los planes institucionales para atender los requerimientos de las entidades de supervisión.

Fuente: elaboración propia

Factores	Riesgos	Oportunidades

3.2 Planificación estratégica

La planificación estratégica implica una fase preparatoria que inicia con el informe de evaluación del organismo de control de la IES. La institución toma dichas observaciones y de esta manera construir las estrategias de avance hacia el cumplimiento normativo de los siguientes años. Uno de los objetivos estratégicos generales debe ser transversal y estar alineado completamente al cumplimiento normativo del organismo de control en simultáneo con la misión y la visión institucional. El objetivo estratégico de cumplimiento debe ir proyectándose al futuro, de tal manera que sea sostenible en el tiempo.

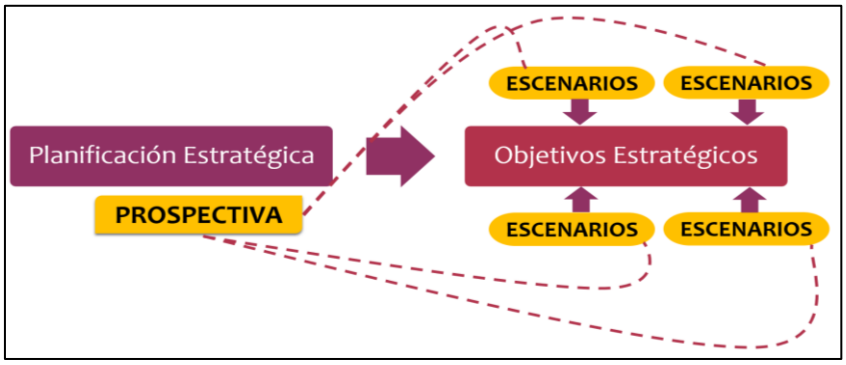
La construcción del Plan Estratégico de Desarrollo Institucional (PEDI), es vital en el tema relacionado con la planeación institucional, el cual que debe ser aprobado por la máxima autoridad de la IES, este deberá ser muy claro y fácil de desarrollar por las autoridades presentes o futuras. El funcionamiento institucional del PEDI corresponde a la configuración consensuada con todas las áreas de la institución de educación superior, de igual manera a ser publicado, socializado y puesto en práctica en la IES. Al establecerse como un modelo de gestión de tecnologías que garantice la fiabilidad y seguridad de repositorios digitales de información debe manejarse como un proyecto combinado, el cual se maneje desde el nivel estratégico al operativo, determinando un alcance específico, en cuyo caso estará orientado a la seguridad de los datos.

Como resultado de la planificación estratégica se debe establecer un objetivo determinante orientado a mejorar la gestión institucional, asegurando la calidad y mejora continua del proceso, enfocado en la gestión de seguridad de la información institucional.

3.3 Prospectiva estratégica

Una vez definido, en la etapa de planificación estratégica, el objetivo determinante e enfocado en la gestión de seguridad de la información académica, el resultado decantará en planes y estrategias que busquen el cumplimiento del mismo; se debe tomar en cuenta que dicho objetivos se irán desarrollado en la medida de las posibilidades en un conjunto de escenarios los cuales pueden ser de tipo políticos, financieros, y de sanidad, como ocurrió en el año 2020 (COVID-19), gracias a la declaración de pandemia por parte de la Organización Mundial de la Salud (Organización Panamericana de la Salud [OPS], 2020), los cuales pueden afectar el cumplimiento de los objetivos establecidos por la institución, figura 6. Una vez revisados los escenarios mencionados, deben analizarse los escenarios alrededor de la consecución de los objetivos estratégicos.

Figura 6. Relación entre planificaciones

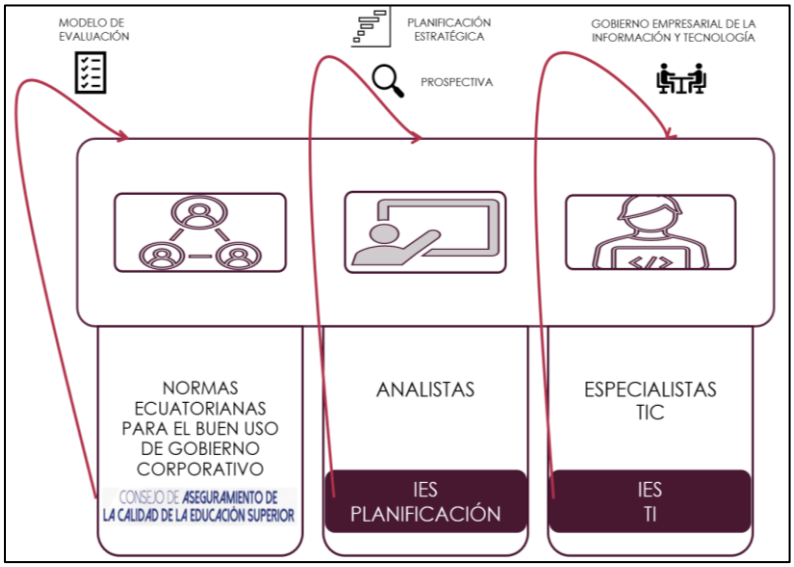


Fuente: elaboración propia

Para realizar el ejercicio de prospectiva estratégica es necesario contar con tres participantes: el grupo de expertos, el cual está conformado por las normas ecuatorianas para el buen uso de gobierno corporativo; el modelo de evaluación a IES del Consejo de Aseguramiento de la Calidad de la Educación Superior y entidades afines; los analistas que constituyen el grupo de Planificación o Calidad de las IES y los especialistas TIC, el cual está conformado por el área de tecnologías de la información del IES.

En una primera etapa, el área de planificación o de calidad analizará los posibles eventos que pueden afectar el cumplimiento del Modelo de Evaluación de Universidades y Escuelas Politécnicas, en cuyo caso corresponde a un "producto de la discusión de la propuesta trabajada por la Comisión Permanente de Evaluación Institucional del CACES" (Caces, 2011, p. 11). En esta etapa quedará claro el objetivo estratégico que será desarrollado en concordancia con la gestión de seguridad de la información académica. Como resultado del análisis, se debe consensuar con el área de tecnologías de la información la posible materialidad de los eventos de riesgo presentados y establecer las posibles soluciones para los eventos presentados en el análisis tal y como lo indica la figura 7.

Figura 7. Prospectiva Estratégica



Fuente: elaboración propia

Capítulo IV. Estructura organizacional

4.1 Gobierno corporativo

El COSO, integrado por "American Accounting Association (AAA), American Institute of CPAs (AICPA), Financial Executives Internacional (FEI), The Association of Accounts and Financial Executives Internacional (FEI), The Association of Accountants and Financial Professional in Business (IMA), The Institute of Internal Auditors (IIA)" (Instituto de Auditores Internos de Colombia, s.f., párr. 6), establece las principales directivas para la creación, gestión y control de un sistema de Control Interno y administración de riesgos. COSO permite que la cultura organizacional pueda ser analizada desde diversas perspectivas, principalmente de quienes deben identificar y administrar los riesgos en una organización, se encarga del control interno de las organizaciones y de la gestión de riesgos empresariales, considerando la importancia de que el modelo de gestión tecnológica propuesto cuente con un proceso de seguridad con relación a la consecución de objetivos relacionados con las operaciones, la información y el cumplimiento.

4.1.1 Arquitectura de control

Arquitectura de control es un concepto que comprende la administración de toda la institución en materia de ambiente de control, gestión de riesgos, sistemas de control interno, información, comunicación, y supervisión de las actividades de la IES. Este sistema general permite a la organización mantener una estructura organizacional que abarca las políticas y procedimientos ejercidos por todos sus integrantes, las cuales cumplen con los debidos estándares de calidad desde el nivel estratégico hasta el operativo (figura 8).

Figura 8. El cubo de COSO

Fuente: (COSO, 2021)

4.2 Gobierno empresarial de la información y tecnología

La integración de tecnología digital en varios ámbitos empresariales fortalece el concepto de información y tecnología (I&T), donde es primordial para el soporte, la sostenibilidad y el crecimiento de las empresas. En el pasado, "la alta gerencia podía delegar, ignorar o evitar las decisiones relacionadas con la información y la tecnología" (Puentes, s.f., párr. 1), mientras que, actualmente el alto nivel de digitalización de las empresas, la eficiencia de procesos, nuevos modelos de negocio e innovación generan el criterio de "creación de valor", el cual es la capacidad corporativa de generar riqueza o utilidad como objetivo empresarial, la importancia de la I&T está directamente relacionada con "la gestión de riesgo empresarial y la generación de valor" (p. 2). El gobierno empresarial de tecnologías de la información (GETI), es parte fundamental del gobierno corporativo, el cual es practicado por la alta dirección encargada de supervisar la definición e implementación de procesos y estructuras, para intersecar a la

organización y al área tecnológica en el desempeño de responsabilidades de alineamiento tecnológico, a partir de la creación de valor del negocio (figura 9).

Figura 9. El contexto del gobierno empresarial de la información y tecnología.

Fuente: COBIT (2019)

4.3 Sistema de gobierno de tecnologías de la información

Las organizaciones implementan gobierno empresarial porque necesitan integrar las tecnologías informáticas al negocio. El concepto de alineamiento estratégico está relacionado con la implementación del modelo de gestión tecnológica que garantice la fiabilidad y seguridad de los repositorios digitales de información de las instituciones de educación superior, donde el objetivo primordial es que las tecnologías de la información generen valor al negocio, convirtiéndolas en un medio por el cual se pueda llegar al cumplimiento de los objetivos empresariales.

Las áreas de tecnologías de la información funcionan dentro de la estructura organizacional de una IES como un terreno de apoyo, mientras que el área de negocio trabaja en un ámbito diferente, motivo por el cual se producen silos de información. En la medida que el grupo tecnológico trabaja en sus proyectos internos el área de negocio no tiene visibilidad del valor que generan los planes de tecnologías de la información, debido a esto se producen diferencias entre las dos áreas, una al no sentirse apoyada en la creación o innovación de

productos o servicios mientras que la otra decide no mostrar asistencia en el cumplimiento de los objetivos planteados.

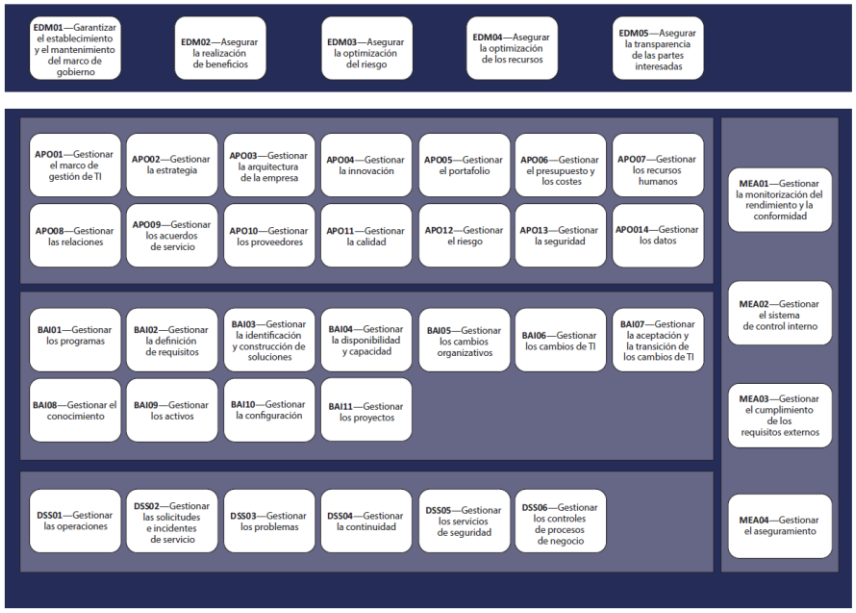
Para lograr empatía entre las áreas del negocio y de tecnología es necesario implementar el enfoque de gobierno de tecnologías de la información, es decir lograr que ambas estén alineadas entre sí., esto hace referencia a todo aquello que sea planificado por el grupo técnico sea porque constituye una necesidad institucional y no debido a que se presenta como una iniciativa sin justificación por parte del responsable del área encargada.

Resulta claro que para la implementar un gobierno de tecnologías de información, gobierno empresarial de tecnologías de información o gobierno corporativo de tecnologías de información, inclusive para las guías actuales de la Asociación de Auditoría y Control de Sistemas de Información (ISACA), se requiere pensar en que la información y la tecnología son el punto más importante, puesto que constituyen el medio a través del cual se logra condensar el contenido que dotará de valor al negocio. La manera de implementar ese enfoque de gobierno empresarial de tecnologías de la información o gobierno corporativo de tecnologías de la información es utilizando un marco de referencia, el cual se basa en una disciplina que incluye las mejores prácticas, guías y herramientas, las cuales permiten alcanzar un objetivo. Entonces contar con el marco de referencia de COBIT, siendo este un marco de referencia de gobierno empresarial de tecnologías de información permitirá implementar en las IES el enfoque de gobierno, es decir buscar alineamiento y generar valor a la institución. En la figura 8, se pueden observar los principales elementos de la arquitectura que lo componen.

El elemento central es el modelo de referencia de COBIT, el cual está formado por un conjunto de objetivos, dentro de los cuales se destacan: de gobierno y de gestión. Por

consiguiente, el COBIT está conformado a su vez por cinco pilares: el primero corresponde al de gobierno, el cual consiste en asegurar el establecimiento y el mantenimiento del marco de gobierno (EDM01), los otros cuatro de gestión procuran: asegurar la entrega de beneficios (EDM02), asegurar la optimización del riesgo (EDM03), asegurar la optimización de recursos (EDM04), asegurar la participación de las partes interesadas (EDM05), en conjunto con 35 objetivos adicionales de gestión. Se habla de disciplina de gobierno y de gestión, puesto que involucran escenarios y momentos que las complementan; las cuales serán explicadas a detalle en lo posterior de este documento. En la figura 10 se observan todos los dominios de gobierno y gestión del marco de referencia COBIT 2019.

Figura 10. Modelo Core de COBIT

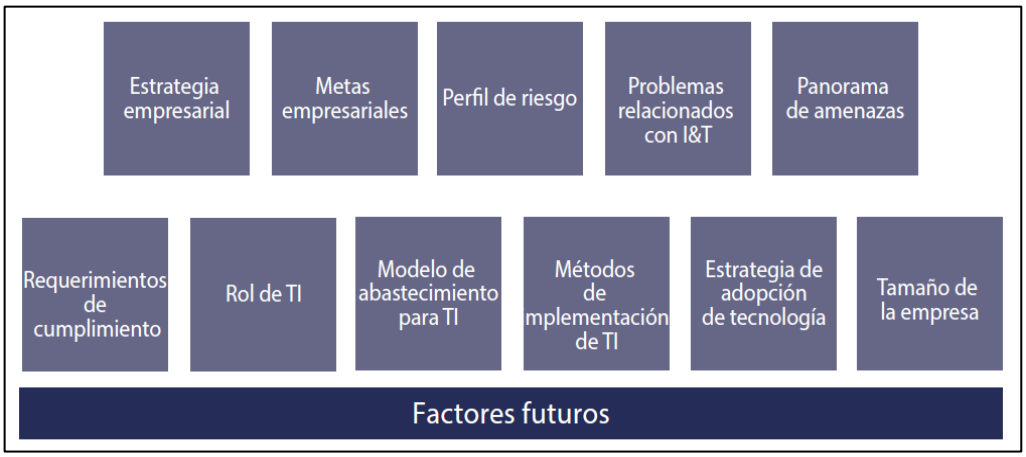


Fuente: COBIT (2019)

Los factores de diseño representan otro elemento de gran importancia para este marco de trabajo, los cuales permiten diseñar el sistema de gobierno empresarial de tecnologías de la

información de forma personalizada y a la medida de cada IES. Los once factores de diseño se pueden apreciar en la figura 11.

Figura 11. Factores de diseño



Fuente: COBIT (2019)

Dentro de los elementos importantes de este marco de trabajo, que se deben considerar para la construcción de un modelo de gestión de tecnologías de información son las denominadas áreas prioritarias, en cuyo caso conservan intereses específicos como por ejemplo la seguridad, riesgo, desarrollo y operaciones (DevOps), en las cuales se pueden implementar los objetivos de gobierno y gestión.

Los objetivos anteriormente descritos son de carácter genérico, es decir que son aplicables ante cualquier escenario, a diferencia de las áreas prioritarias que están orientados a un tema en particular; dentro de estas últimas mencionadas se encuentra la seguridad de la información, la cual constituye un eje transversal en el desarrollo del presente trabajo.

En relación con lo expuesto previamente, el modelo de gestión tecnológica que garantice la fiabilidad y seguridad de repositorios digitales de información de IES estará conformado por la

fase de planificación en suma con la fase de gobierno de tecnologías de la información, orientada principalmente en los factores de diseño y en las áreas prioritarias.

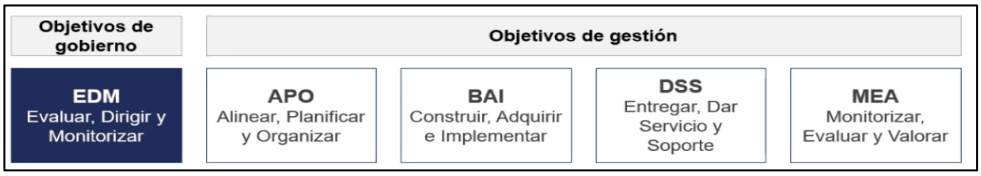
4.4 Objetivos de gobierno y gestión

El modelo de referencia COBIT está basado en los objetivos de gobierno y los objetivos de gestión, los cuales constituyen un elemento importante del modelo, dentro de esta estructura existe cuarenta objetivos, los cuales están organizados por dominios, de ahí que tenemos un dominio de Gobierno y cuatro dominios de Gestión, como se puede observar en la figura 12.

Los objetivos de gobernanza se agrupan en el dominio EDM (Evaluar, Dirigir y Monitorizar). En este dominio, el organismo de gobierno evalúa las opciones estratégicas, dirige a la alta dirección sobre las opciones estratégicas elegidas y supervisa el logro de la estrategia. Los objetivos de gestión se agrupan en cuatro dominios.

- Alinear, Planificar y Organizar (APO). - aborda la organización de manera general, la estrategia y las actividades de apoyo para la información y tecnología.
- Construir, Adquirir y Organizar (BAI). – como especifica su nombre, está relacionado con la adquisición e implementación de soluciones de integración para la información y tecnología en los procesos de negocio.
- Entregar, Dar Servicio y Soporte (DSS). - aborda la prestación operativa y el soporte de los servicios de información y tecnología, incluida la seguridad.
- Monitorizar, Evaluar y Valorar (MEA). - aborda el monitoreo del desempeño y la conformidad de información y tecnología con metas de desempeño interno, objetivos de control interno y requisitos externos.

Figura 12. Objetivos de gobierno y gestión.



Fuente: Marco de referencia COBIT 2019.

Los nombres de los dominios están identificados por los verbos que producen las acciones a realizar dentro de cada uno, por ejemplo el objetivo de gobierno tiene como dominio (se convierte en dominio de gobierno) EDM que está encargado de evaluar, dirigir y monitorizar, lo que significa que este dominio tiene el propósito de evaluar el sistema de gobierno de la organización; dirigir, en lo referente a proporcionar las directrices, políticas y estrategias de gobierno; y monitorizar, en lo referente a supervisión de que todas las estrategias y el cumplimiento de políticas.

La responsabilidad del cumplimiento de este dominio recae en la alta Dirección de la IES, o en la estructura organizacional que asuma las responsabilidades de la Dirección, para el caso de nuestro estudio puede constituirse en el Consejo Universitario, Consejos Directivos, u otro órgano colegiado. En cuanto a la gestión, el marco de gobierno nos proporciona cuatro dominios que están organizados de la siguiente manera: APO, que está relacionado con “alinear, planificar y organizar, BAI que está relacionado con construir, adquirir e implementar, DSS está relacionado con entregar, proporcionar servicio y soporte, MEA está enfocado en monitorizar evaluar y valorar”.

Dentro de cada uno de los dominios antes nombrados, podemos encontrar los objetivos. En los objetivos de gobierno se encuentran las tareas, las mismas que tiene que desarrollar la alta

dirección de la IES, en el caso de nuestro estudio, estas tareas las tiene que realizar el órgano colegiado institucional, quien tiene a su responsabilidad, las actividades de dirección y control de tecnologías de información, en resumen, el órgano colegiado de la IES debe dirigir y controlar el ámbito relacionado con las tecnologías de información y comunicaciones, como por ejemplo, la alta Dirección de la IES, tiene que dirigir las estrategias, las políticas, validar la gestión de riesgos, para que pueda exponer que, el área de tecnologías de la información está generando beneficios a la institución, como por ejemplo en la optimización o reutilización de recursos tecnológicos.

De acuerdo con el marco de gobierno aplicado, el cumplimiento de los objetivos de gobierno de gestión corresponde a todas las áreas de la IES. En este nuevo escenario el responsable máximo de tecnologías de información se convierte el rector de la IES, y todas las áreas a su mando participan en la gestión, con relación a la gestión, todas las áreas que conforman la IES, es decir coordinaciones, direcciones, o como se encuentren definidas en el organigrama de la IES, deben seguir las directivas de los objetivos de gobierno organiza todos los elementos de tecnología de la información con el dominio "APO (Alinear, Planificar y Organizar), construye las soluciones del negocio que requiere BAI (Construir, Adquirir e Implementar)" (Salah, 2017, p. 16), entrega esas soluciones a través del dominio DSS (Entregar, Dar Servicio y Soporte), y monitoriza y supervisa que todo funcione bien a través de los objetivos del dominio MEA (Monitorizar, Evaluar y Valorar). Es así como funciona este modelo de gobierno de tecnologías de la información, que será adaptado por la IES.

4.5 Componentes de un sistema de gobierno

Para implementar el modelo de gestión de tecnológica que garantice la fiabilidad y seguridad de los repositorios digitales de información de instituciones de educación superior, la IES tiene que diseñar un sistema de gobierno a través de los objetivos de gobierno de gestión seleccionados, tomando en cuenta el perfil de seguridad de la información, lo que avale la seguridad de los datos almacenados en los repositorios de información institucional.

Los componentes son factores que, individual y colectivamente, contribuyen al buen funcionamiento del sistema de gobernanza sobre la información y tecnología de la IES. Los componentes interactúan entre sí, lo que resulta en un sistema de gobernanza integral para la información y tecnología. Los componentes pueden ser de diferentes tipos, como se observa en la figura 13.

Figura 13. Componentes COBIT de un sistema de gobierno.

Fuente: Marco de referencia COBIT 2019.

Los más familiares son los procesos. Sin embargo, los componentes de una gobernanza también incluyen estructuras organizativas, políticas, procedimientos, elementos de información; cultura, comportamiento, destrezas, competencias, servicios, infraestructura y aplicaciones. Para

satisfacer los objetivos de gobernanza y gestión, la IES necesita establecer, adaptar y mantener una gobernanza a partir de los siguientes componentes:

- **Principios, políticas y marcos. -** están relacionados en la gestión del comportamiento diario.
- **Procesos. –** "describen un conjunto organizado de prácticas y actividades para lograr ciertos objetivos y producir un conjunto de productos que respaldan el logro de los objetivos generales relacionados con las tecnologías de la información" (Ceupe Magazine, s.f., párr. 2).
- **Estructuras organizacionales. -** Las estructuras organizativas son las entidades clave para la toma de decisiones en la institución.
- **La cultura, la ética y el comportamiento. -** "La cultura, la ética y el comportamiento de las personas y de la empresa a menudo se subestiman como factores de éxito en las actividades de gobernanza y gestión" (párr. 4).
- **La información. -** es omnipresente en cualquier organización e incluye toda la información producida y utilizada por la empresa. COBIT se enfoca en la información requerida para el efectivo funcionamiento del sistema de gobernanza de la empresa.
- **Los servicios, la infraestructura y las aplicaciones. -** "incluyen la infraestructura, la tecnología y las aplicaciones que proporcionar a la empresa el sistema de gobierno para el procesamiento de la información y tecnología" (párr. 6).

- **Personas, habilidades y competencias. -** son requeridas para la toma de buenas decisiones, ejecutar acciones correctivas y finalización exitosa de todas las actividades.

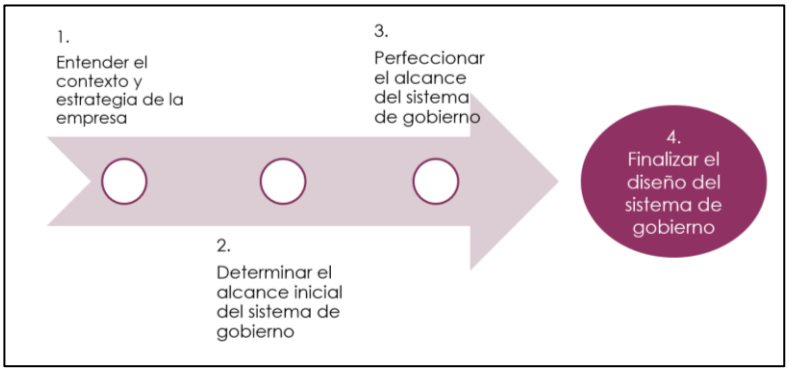
Para cumplir con la propuesta de un modelo de gestión de tecnologías de información que garantice la fiabilidad y seguridad de repositorios digitales de información de instituciones de educación superior, es necesario diseñar un sistema de gobierno, y la manera de implementar este sistema de gobierno es a través de los objetivos de gobierno de gestión, motivo por el cual serán seleccionados los puntos más relevantes del universo de controles que se encuentran definidos dentro del marco de gobierno de tecnologías de la información, velando porque estos cubran los aspectos relacionados con la seguridad de los repositorios digitales.

El éxito de este tipo de modelos está basado en un proceso de mejora continua. El enfoque sistémico se fundamenta en percibir a la empresa como un sistema constituido por diferentes procesos interrelacionados entre sí gracia a la visión, misión, valores y objetivos estratégicos; la actitud preventiva se aprecia a través de la estructura de los requisitos, ya que estos siguen el modelo de gestión sugerido por Edwards Deming: planificar, hacer, verificar y actuar; dentro de los cuales se entiende el“ actuar” como “mejorar”; es decir, tales modelos promueven la mejora continua de los procesos (Díaz et al., 2020).

4.6 Factores de diseño

Para el presente trabajo es necesario caracterizar los factores de diseño; para delinear el sistema de gobierno es necesario contar con un flujo de trabajo constituido por cuatro pasos, tal y como lo indica la figura 14.

Figura 14. Factores de diseño.



Fuente: Marco de referencia COBIT 2019.

Factor de diseño 1. El primer paso del diseño es comprender el contexto y la estrategia de la empresa; posteriormente se examinan los fundamentos de ambas nociones y se plantea la relación existente en el entorno empresarial de la IES, para lograr un mayor entendimiento de los cuatro primeros factores de diseño (estrategia empresarial, metas empresariales, perfil de riesgo y entender los problemas relacionados con la información y tecnología), que se encuentran parcialmente solapados pero que a su vez son interdependientes y a menudo complementarios.

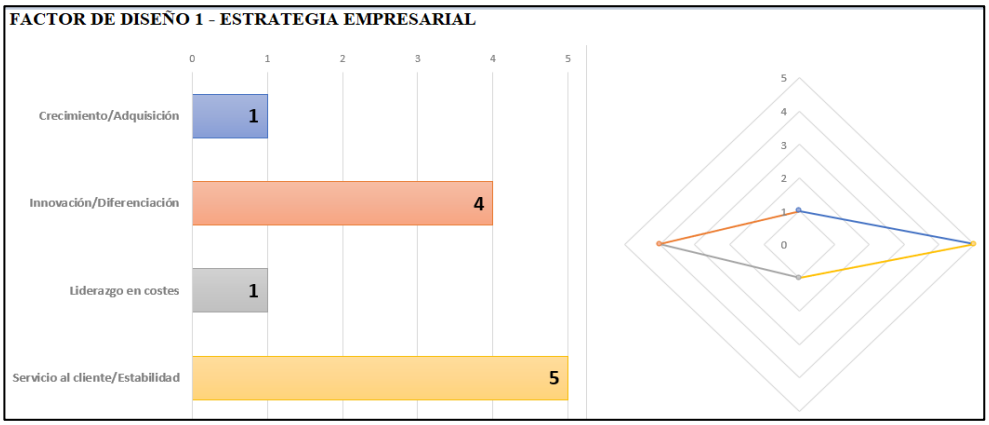
Tabla 3. *Factor de diseño 1 – Estrategia de la empresa*

Arquetipo de la estrategia	Explicación
Crecimiento / Adquisición.	La empresa se centra en el crecimiento (de los ingresos).
Innovación / Diferenciación.	La empresa se enfoca en ofrecer productos y servicios diferentes y/o innovadores a sus clientes.
Liderazgo en costes.	La empresa prioriza la minimización del coste a corto plazo.
Servicio al cliente / Estabilidad.	La empresa busca proporcionar un servicio estable y orientado al cliente.

Fuente: elaboración propia

De acuerdo con la tabla 3, la estrategia primaria identificada se encuentra dentro del marco del servicio al cliente, y como estrategia secundaria se evidencia: Innovación / Diferenciación.

Figura 15. Factor de diseño 1



Fuente: COBIT (2019)

Factor de diseño 2.- La estrategia empresarial "se logra mediante la consecución de metas empresariales. Estas se definen en el marco de referencia de COBIT 2019" (COBIT, 2018, p. 24), donde se estructuran en torno a las dimensiones de un cuadro de mando integral (Balanced Scorecard, BSC).

Tabla 4. *Metas empresariales*

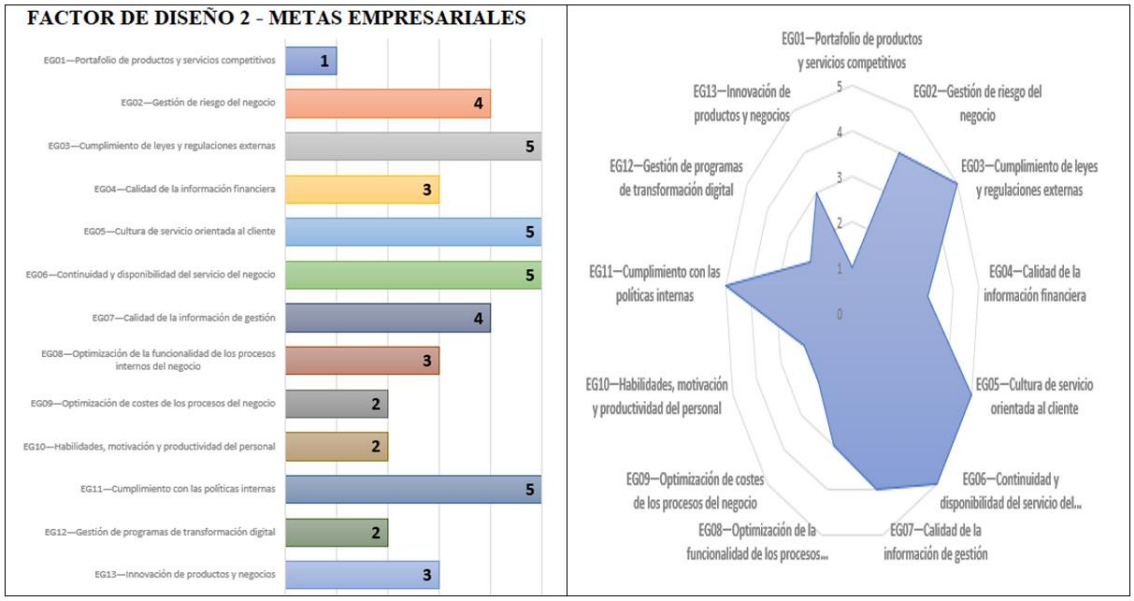
Referencia	Dimensión del cuadro de mando integrado (Balanced Scorecard)	Meta empresarial
EG01	Financiera	Portafolio de productos y servicios competitivos.
EG02	Financiera	Gestión de riesgo del negocio.
EG03	Financiera	Cumplimiento de leyes y regulaciones externas.
EG04	Financiera	Calidad de la información financiera.
EG05	Cliente	Cultura de servicio orientada al

		cliente.
EG06	Cliente	Continuidad y disponibilidad del servicio del negocio.
EG07	Cliente	Calidad de la información de gestión.
EG08	Interna	Optimización de la funcionalidad de los procesos internos del negocio.
EG09	Interna	Optimización de costes de los procesos de negocio.
EG10	Interna	Habilidades, motivación y productividad personal.
EG11	Interna	Cumplimiento de políticas internas.
EG12	Crecimiento	Gestión de programas de transformación digital.
EG13	Crecimiento	Innovación de producto y negocio.

Fuente: elaboración propia

De acuerdo con la tabla 4, las metas empresariales para la IES serán las siguientes: EG03 Cumplimiento de leyes y regulaciones externas, EG05 Cultura de servicio orientada al cliente, EG06 Continuidad y disponibilidad del servicio del negocio, EG11 Cumplimiento de políticas internas. El respectivo análisis se puede observar en la figura 16.

Figura 16. Factor de diseño 2



Fuente: COBIT (2019)

Factor de diseño 3.- Está conformado por el perfil del riesgo, donde COBIT declara que toda institución está sujeta a riesgos dentro de un campo compuesto por 19 categorías, como se puede observar en la figura 17.

Figura 17. Categorías de riesgos

Fuente: COBIT (2019)

Una vez aplicada la metodología de análisis de riesgos (figura 18), se han identificado que los posibles riesgos que pueden producirse en la IES son los incidentes de infraestructura operativa de tecnologías de información, los ataques lógicos (hacking, malware), y los derivados a causa del incumplimiento.

Figura 18. Factor de diseño 3

Categoría del escenario de riesgo	Impacto (1-5)	Probabilidad (1-5)	Clasificación
Toma de decisiones sobre inversiones en TI, definición y mantenimiento del portafolio	2	2	
Gestión del ciclo de vida de los programas y proyectos	4	2	
Coste y control de TI	3	2	
Comportamiento, habilidades y conocimiento de TI	4	2	
Arquitectura de la empresa/TI	4	2	
Incidentes de infraestructura operativa de TI	5	3	
Acciones no autorizadas	4	2	
Adopción de software/problemas de uso	4	2	
Incidentes de hardware	4	2	
Fallos de Software	3	2	
Ataques lógicos (hacking, malware, etc.)	5	5	
Incidentes de terceros/proveedores	2	2	
Incumplimiento	5	4	
Problemas geopolíticos	2	3	
Acción industrial	1	2	
Actos de la naturaleza	3	3	
Innovación basada en la tecnología	5	2	
Medio ambiente	2	2	
Gestión de datos e información	4	3	

	Riesgo muy alto
	Riesgo alto
	Riesgo normal
	Riesgo bajo

Fuente: COBIT (2019)

Factor de diseño 4.- Constituye los problemas relacionados con la información y la tecnología. Está configurado por riesgos que pueden materializarse, para el caso de una IES son los que se indican en la tabla 5.

Tabla 5. *Problemas relacionados con la información y tecnología*

Referencia	Descripción
C	Incidentes significativos relacionados con TI, como pérdida de datos, brechas de seguridad, fracaso de proyectos, errores de las aplicaciones.
E	Incumplimiento de los requisitos regulatorios o contractuales.
S	Incumplimiento de las regulaciones de seguridad y privacidad.

Figura 19. Factor de diseño 4

Fuente: COBIT (2019)

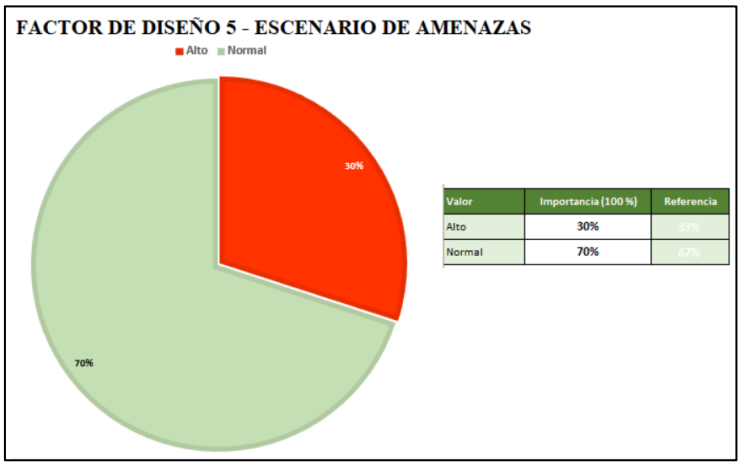
Factor de diseño 5.- Establece los escenarios de amenazas bajo los cuales opera la empresa, estos pueden clasificarse de la siguiente manera:

Tabla 6. *Escenario de amenazas*

Escenario de amenaza	Explicación
Normal	La empresa funciona bajo lo que se consideran niveles de amenaza normales.
Alto	Debido a su situación geopolítica, sector industrial o perfil especifico, la empresa funciona en un escenario de amenazas elevadas.

Para el caso de una IES, el escenario de amenaza es considerado “normal” con un 70 % y alto con un 30 %.

Figura 20. Factor de diseño 5



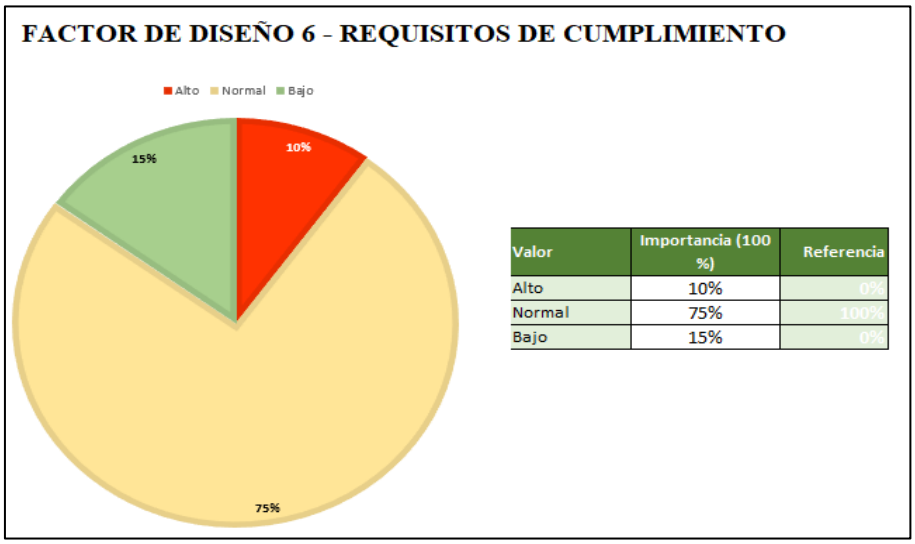
Fuente: COBIT (2019)

Factor de diseño 6.- Formado por los requisitos de cumplimiento a los que la empresa está sujeta, puede clasificarse por medio de un entorno regulatorio de requisitos de cumplimiento normales, de acuerdo con las categorías definidas en la tabla 7.

Tabla 7. *Requisitos de cumplimiento*

Entorno regulatorio	Explicación
Requisitos de cumplimiento bajos	La empresa está sujeta a un conjunto de requisitos mínimos de cumplimiento que son inferiores a la medida.
Requisitos de cumplimiento normales	La empresa está sujeta a un conjunto de requisitos de cumplimiento comunes a las distintas industrias.
Requisitos de cumplimiento altos	La empresa está sujeta a requisitos de cumplimiento más elevados de lo normal, en la mayoría de los casos relacionados con el sector industrial y las condiciones geopolíticas.

Figura 21. Factores de diseño 6.



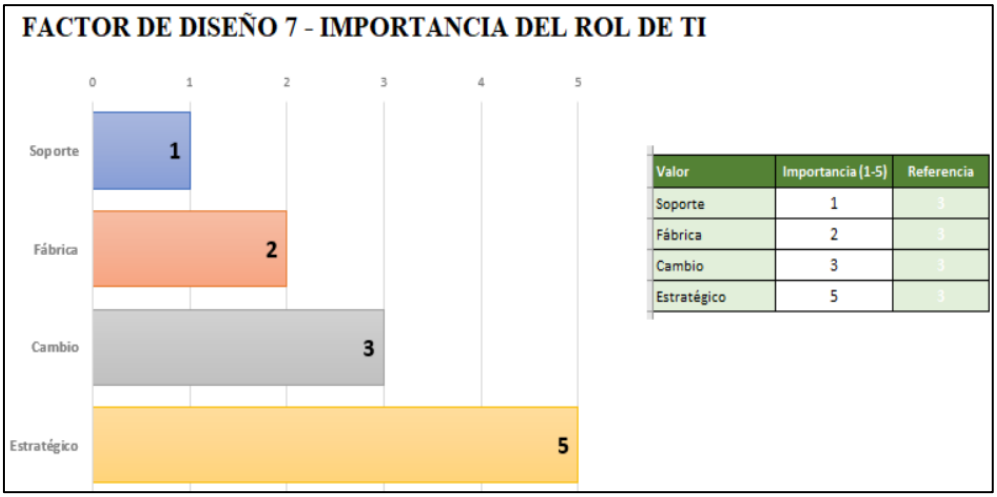
Fuente: COBIT (2019)

Factor de diseño 7.- De acuerdo con los resultados arrojados en la tabla 8, el rol de tecnología de la información en una IES es “estratégico” (figura 22).

Tabla 8. *Rol de TI*

Rol de TI	Explicación
Soporte	TI no es crucial para el funcionamiento y la continuidad de los procesos y servicios del negocio ni para su innovación.
Fábrica	Cuando las TI fallan hay un impacto inmediato en el funcionamiento y continuidad de los procesos y servicios de negocio. Sin embargo, las TI no se consideran un factor impulsor de la innovación en los procesos y servicios del negocio.
Cambio	Las TI se consideran un factor impulsor de la innovación de procesos y servicios del negocio, sin embargo, no hay una dependencia crítica en las TI para el funcionamiento y la continuidad actual de los procesos y servicios empresariales.
Estratégico	Las TI son críticas para el funcionamiento e innovación de los procesos y servicios del negocio de la organización.

Figura 22. Factor de diseño 7



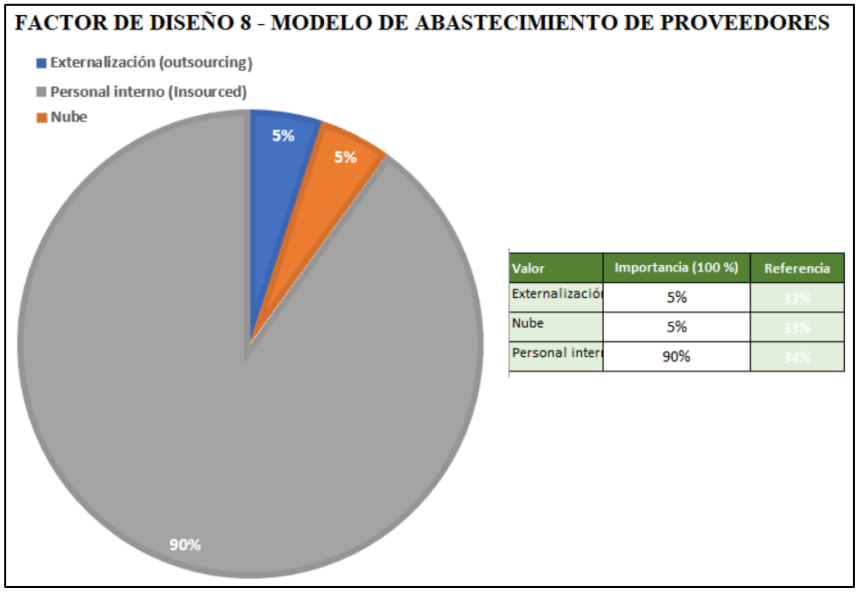
Fuente: COBIT (2019)

Factor de diseño 8.- A partir de lo reflejado en la tabla 9, se concluye que el modelo de abastecimiento para TI es “personal interno”.

Tabla 9. *Modelo de abastecimiento para TI*

Modelo de abastecimiento	Explicación
Externalización	La empresa requiere los servicios de un tercero para proporcionar servicios de TI.
Nube	La empresa maximiza el uso de la nube para proporcionar servicios de TI a sus usuarios.
Personal interno	La empresa aporta personal y servicios propios de TI.
Híbrido	Se aplica un modelo híbrido que combina los otros tres modelos en distintos grados.

Figura 23. Factor de diseño 8



Fuente: COBIT (2019)

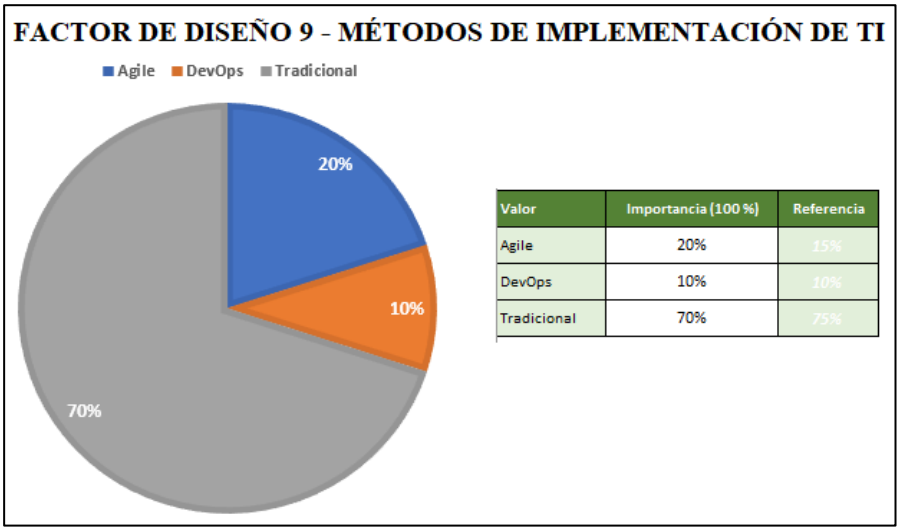
Factor de diseño 9.- El modelo de gestión tecnológica que garantice la fiabilidad y seguridad de repositorios digitales de información de IES, adoptará el modelo de implementación de TI de modo tradicional (para referencia ver tabla 10).

Tabla 10. *Métodos de implementación de TI*

Implementación de TI	Explicación
Agile	La empresa utiliza los métodos de desarrollo de trabajo Agile para su desarrollo de software.
DevOPs	La empresa usa los métodos de trabajo DevOps para la creación, despliegue y operaciones de software.
Tradicional	"La empresa emplea un método más clásico para el desarrollo de software (cascada) y separa el desarrollo de software de las operaciones" (COBIT Diseño, 2019, párr. 12).
Híbrido	La empresa maneja una mezcla de implementación de TI tradicional y TI moderna, a la que solemos referirnos como TI bimodal.

Fuente: elaboración propia

Figura 24. Factor de diseño 9



Fuente: COBIT (2019)

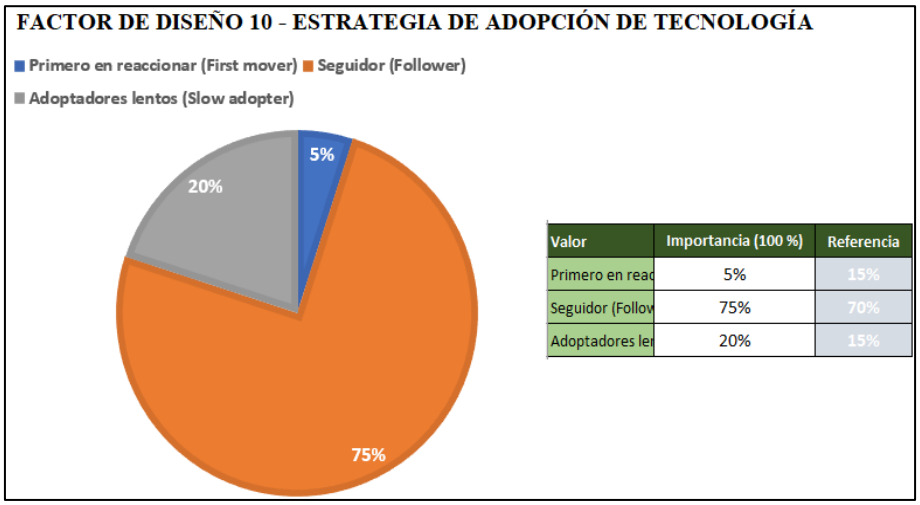
Factor de diseño 10.- En este punto se elige la estrategia de adopción de tecnología que será la designada como seguidor (Follower), como se puede observar en la figura 25.

Tabla 11. *Estrategia de adopción de tecnología*

Estándares de adopción de tecnología	Explicación
Primer entrante (First mover)	La empresa suele adoptar nuevas tecnologías lo antes posible e intenta lograr la "ventaja del primer entrante".
Seguidor (Follower)	La empresa suele esperar a que las nuevas tecnologías se generalicen y las pongan a prueba antes de adoptarlas.
Adoptadores lentos (Slow adopter)	La empresa tarda mucho en adoptar las nuevas tecnologías.

Fuente: elaboración propia

Figura 25. Factores de diseño 10



Fuente: COBIT (2019)

Factor de diseño 11.- El diseño de un sistema de gobierno de la empresa estará enfocado en las empresas grandes.

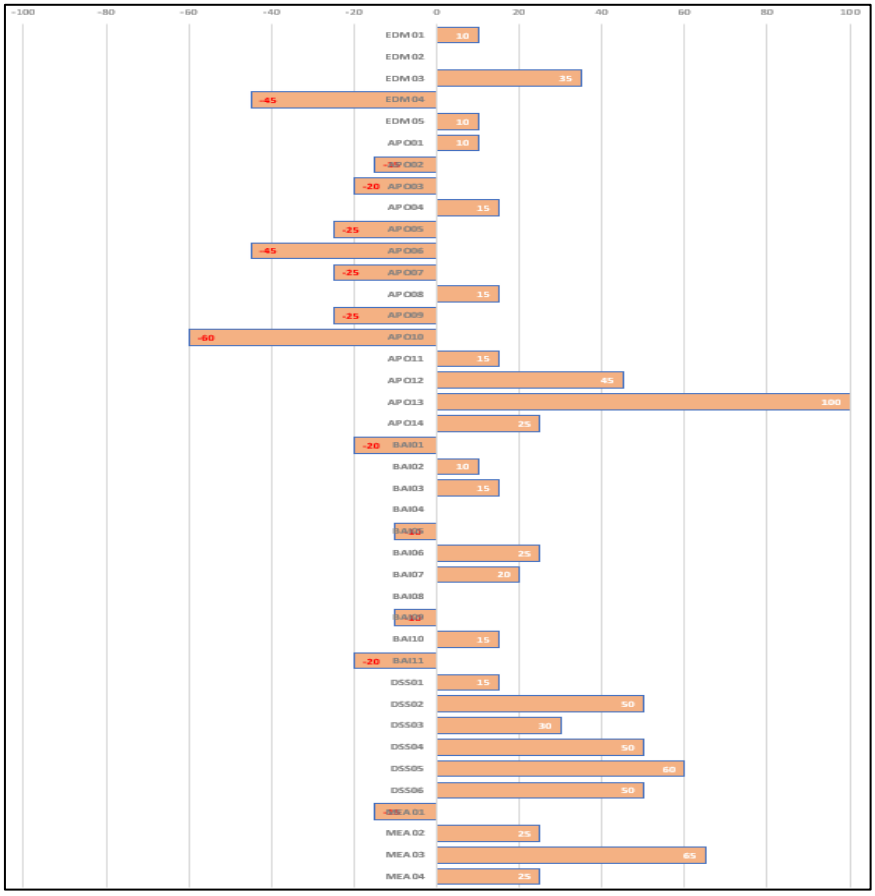
Tabla 12. *Factor de diseño, tamaño de la empresa*

Tamaño de la empresa	Explicación
Empresa grande (predeterminada)	Empresa con más de 250 empleados a tiempo completo.
Pequeñas y medianas empresas	Empresa entre 50 y 250 empleados que laboran a tiempo completo (FTE).

Fuente: elaboración propia

En la figura 26, se visualiza el análisis al aplicar todos los factores de diseño, en la que se muestra como resultado: la implementación del proceso APO13, para gestionar la seguridad.

Figura 26. Todos los factores de diseño

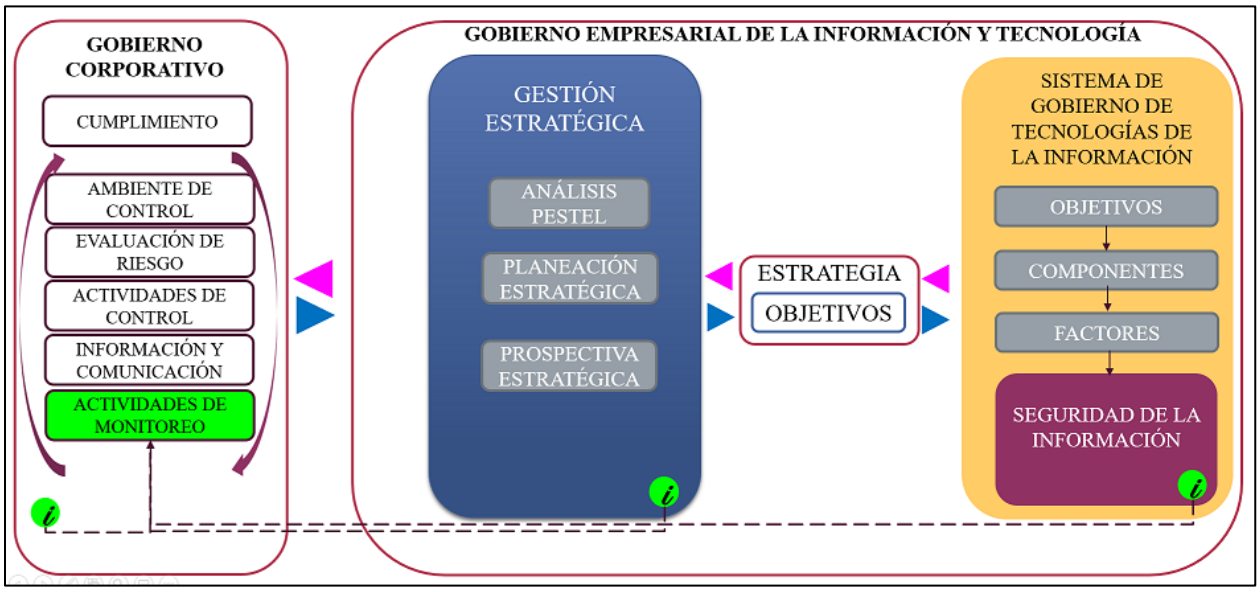


Fuente: COBIT (2019)

Capítulo V. Descripción del modelo de gestión tecnológica que garantice la fiabilidad y seguridad de repositorios digitales de información

El modelo de gestión tecnológica que garantice la fiabilidad y seguridad de repositorios digitales de información de una IES está compuesto por la integración de dos grupos que conforman el modelo, el gobierno corporativo y el gobierno empresarial de la información y tecnología, los cuales van interactuando con base a la necesidad de cumplimiento normativo, lo que genera una interacción entre estos dos grandes componentes, esto se logra apreciar en la figura 27.

Figura 27. Modelo de gestión de tecnologías de la información



Fuente: elaboración propia

5.1 Gobierno corporativo

En esta sección del modelo estará determinado por la arquitectura de control, la cual incluye la gestión de riesgos, sistemas de control interno, información, comunicación, y monitoreo de la gestión operativa de la IES, gracias a que permite contar con un sistema holístico que permitirá utilizar una estructura, políticas y procedimientos ejercidos por todos los integrantes de la institución, entiéndase desde el nivel gerencial hasta el nivel operativo. Se formará entonces, el Comité de Riesgos que será el responsable de determinar el alcance de los principales riesgos operacionales que pudiesen surgir, mismos que puedan afectar la consecución de los objetivos estratégicos. Este comité formulará un informe con las recomendaciones que le competen a la máxima autoridad de la IES. El sistema de control interno estará basado en los componentes de COSO, de la siguiente manera:

5.1.1 Ambiente de control

Está relacionado con la cultura organizacional, en el cual la IES debe fomentar los principios y valores institucionales. Los objetivos estratégicos deben estar alineados con la misión, visión y los objetivos estratégicos.

5.1.2 Evaluación de riesgos

La IES y sus partes interesadas críticas han evaluado las operaciones, informes y objetivos de cumplimiento y se ha recopilado información para comprender cómo la deficiente gestión de seguridad de la información puede afectar a los objetivos institucionales.

5.1.3 Actividades de control

La IES tiene la tarea de desarrollar actividades de control, incluyendo las ejercidas en materia de tecnología, que les permitan gestionar los riesgos de seguridad dentro del nivel de tolerancia aceptable para la institución. Es necesario que estas actividades se implementen de acuerdo con políticas y procedimientos formalizados.

5.1.4 Información y comunicación

La IES identificará los requisitos de información para gestionar el control interno relacionado con el riesgo de seguridad de la información. La institución ha definido canales y protocolos de comunicación internos y externos que apoyen el funcionamiento del control interno. Definir los planes de continuidad de negocio donde debe incluir el árbol de comunicación de la institución.

5.1.5 Actividades de monitoreo

El monitoreo se realizará tomando en cuenta los indicadores definidos en los componentes del modelo de gestión tecnológica definidos en este capítulo, lo que servirá para determinar la efectividad operativa de los controles internos que abordan los riesgos de seguridad, esto también permitirá identificar las deficiencias, para que de esta manera se logren tomar a tiempo los correctivos necesarios en cada etapa del modelo.

5.1.6 Cumplimiento

El cumplimiento normativo o también conocido en el ámbito empresarial como “Compliance”, tiene la función de garantizar el respeto por las normas o políticas internas,

velando por el cumplimiento de las mismas con base en las leyes vigentes, las cuales son supervisadas por un organismo de control, en este caso el cumplimiento del Modelo de Evaluación de Universidades y Escuelas Politécnicas, del CACES. Esta sección del modelo se encarga de asesorar, vigilar y monitorizar los riesgos de posibles incumplimientos legales en la IES.

La finalidad del cumplimiento normativo se basa en ejecutar los aspectos o controles que requieren los entes de control externo como por ejemplo el CACES, o controles internos como puede ser los diferentes Comités institucionales, para la creación de directrices institucionales enfocadas en buscar la forma adecuada de adaptarse a las diferentes normativas.

El cumplimiento deberá ser una política institucional conocida por todos los integrantes de la IES. Las funciones del cumplimiento normativo son las siguientes:

Prevención. - Impedir los riesgos. Es necesario identificar los posibles riesgos de incumplimiento del Modelo de Evaluación de Universidades y Escuelas Politécnicas, e informar a los empleados y directivos de una IES.

Detección. - Encontrar las carencias en los "controles de cumplimiento de las normas".

Informar. - Comunicar permanentemente a la alta dirección sobre los riesgos de incumplimiento del Modelo de Evaluación de Universidades y Escuelas Politécnicas, y los planes de acción que se propondrán para su cumplimiento.

En la tabla 13 se encuentra definido el indicador de gobierno corporativo, el cual corresponde a un indicador de efectividad que mide la capacidad de los procesos auditados enfocado en la búsqueda de un efectivo control interno de todo el modelo.

Tabla 13. *Indicador Gobierno Corporativo.*

Nombre del indicador	Impacto de las recomendaciones realizadas
Tipo de indicador	Efectividad.
Descripción	Mide la capacidad de los procesos auditados para autocontrolarse y genera mejora.
Proceso	Control interno.
Fórmula	(Recomendaciones acatadas / Recomendaciones realizadas). *100
Unidades	%
Meta	95 %
Tendencia esperada	Mantener.
Frecuencia de medición	Anual.
Fuente de información	Informes de auditoría interna.
Área responsable	Responsable del control interno de la IES.

Fuente: elaboración propia

5.2 Gobierno empresarial de la información y tecnología

5.2.1 Gestión estratégica

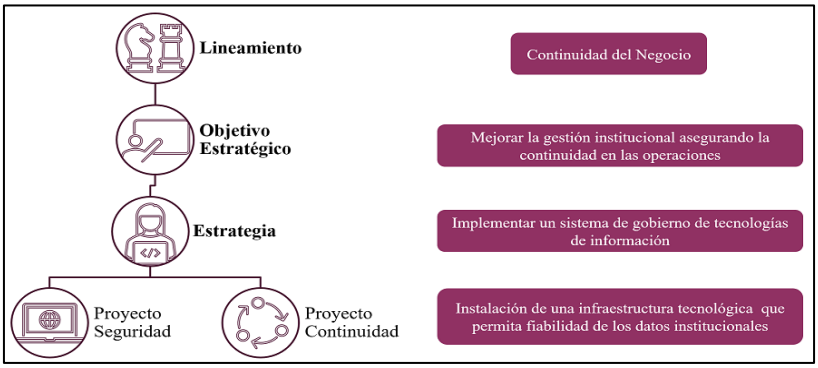
La gestión estratégica define la orientación del negocio y provee las herramientas para progresar en la dirección que ha escogido la IES. En esta sección se incorporan dos elementos, los cuales interactúan entre sí, en esta fase se trabaja en coordinación con la definición y la ejecución, donde se convierte en una relación dependiente (la una de la otra). En el libro "El arte de la ejecución en los negocios", se indicó que "la ejecución es una disciplina olvidada por la mayoría de las empresas. No es un conjunto de tácticas, es la habilidad de llevar a la práctica la estrategia planeada" (Charan y Bossidy, 2003, p. 216), a partir de dicho principio se hace evidente la importancia de que la estrategia definida sea puesta en práctica gracias a la adopción de este modelo, en el cual debe existir la definición estratégica que incluya la misión, visión, valores, estrategia. Posteriormente, establecer los objetivos estratégicos a corto, mediano o largo

plazo, para este caso de estudió el tiempo responderá al delimitado como corto plazo debido al ciclo de revisión por parte del organismo de control. El objetivo estratégico estará enfocado en el proceso de gestión de la seguridad de la información, de esta manera, se puede mejorar eficiencia en el proceso o mejorar el nivel de calidad del mismo.

Estrategia. - La estrategia definida será auspiciada por la Dirección de la IES, dado que está orientada a la infraestructura y equipamiento informático con un enfoque de procesos. Esta estrategia estará definida por uno de los elementos fundamentales de la función sustantiva del Modelo de Evaluación de Universidades y Escuelas Politécnicas, del Consejo de Aseguramiento de la CACES las cual dicta que "La institución cuenta con una plataforma informática disponible y accesible a la comunidad universitaria para la gestión de los procesos académicos y administrativos" (Caces, 2019).

Dentro de los propósitos de la estrategia definida se busca establecer el objetivo estratégico de manera clara y concisa, que sirva de guía para entender el desplazamiento de esta, desde el nivel estratégico hasta el operacional. La estrategia está definida en la figura 28.

Figura 28. Estrategia



Fuente: elaboración propia

Esta área genera el indicador de gestión estratégica, el cual será reportado al grupo de Gobierno Corporativo y será evaluado en las actividades de monitoreo. El indicador se detalla en la siguiente tabla.

Tabla 14. *Indicador Gestión Estratégica.*

Nombre del indicador	Impacto de las recomendaciones realizadas
Tipo de indicador	Efectividad,
Descripción	Mide la capacidad de los procesos auditados para autocontrolarse y genera mejora,
Proceso	Control interno,
Fórmula	(Recomendaciones acatadas / Recomendaciones realizadas),*100
Unidades	%
Meta	95 %
Tendencia esperada	Mantener.
Frecuencia de medición	Anual.
Fuente de información	Informes de auditoría interna.
Área responsable	Responsable del control interno de la IES.

Fuente: elaboración propia

5.2.2 Sistema de gobierno de tecnologías de la información

El sistema de gobierno de tecnología de la información se encuentra detallado en el capítulo anterior, este ítem está encauzado en el proceso de gestión de la seguridad APO13, cuyo propósito es disminuir el impacto de los incidentes de seguridad de la información dentro de los niveles aceptables de riesgo de la IES; los cuales fueron definidos por el Gobierno Corporativo.

Dentro de un contexto de mejora continua se debe mantener la comunicación periódica de las actividades relacionadas con la seguridad de la información. Trabajar en función de establecer un sistema de gestión de seguridad de la información (SGSI), mejorar su eficacia, establecer indicadores y corregir las no conformidades para evitar que se repitan. Para el acatamiento del modelo propuesto en este estudio se han definido indicadores de gestión y cumplimiento, los cuales se describen a continuación.

Tabla 15. *Indicador de impacto de las recomendaciones realizadas*.

Nombre del indicador	Impacto de las recomendaciones realizadas
Tipo de indicador	Gestión.
Descripción	Determina la eficiencia en el tratamiento de eventos relacionados a la seguridad de la información.
Proceso	Control interno.
Fórmula	(Número de anomalías cerradas / Número total de anomalías encontradas). *100
Unidades	%
Meta	90 %
Tendencia esperada	Mantener.
Frecuencia de medición	Semestral.
Fuente de información	Informes de auditoría interna.
Área responsable	Responsable del área tecnológica o seguridad de la información (depende de la estructura de la IES).

Fuente: elaboración propia

Tabla 16. *Indicador de verificación de control de acceso*.

Nombre del indicador	Verificación de control de acceso
Tipo de indicador	Cumplimiento.
Descripción	Identifica la existencia de lineamientos, normas o estándares en cuanto al control de acceso a la información.
Proceso	Seguridad.
Fórmula	(Políticas acatadas / Políticas realizadas). *100
Unidades	%
Meta	>=90 %
Tendencia esperada	Mantener.
Frecuencia de medición	Semestral.
Fuente de información	Usuarios internos.
Área responsable	Responsable del área tecnológica o seguridad de la información (depende de la estructura de la IES).

Fuente: elaboración propia

Tabla 17. *Indicador de implementación de controles de seguridad.*

Nombre del indicador	Implementación de controles de seguridad
Tipo de indicador	Gestión.
Descripción	Identifica el grado de avance en la implementación de controles de seguridad.
Proceso	Seguridad.
Fórmula	(Número de controles implementados / Número de controles planificados). *100
Unidades	%
Meta	>=90 %
Tendencia esperada	Mantener.
Frecuencia de medición	Semestral.
Fuente de información	Plan de tratamiento de riesgos.
Área responsable	Responsable del área tecnológica o seguridad de la información (depende de la estructura de la IES).

Fuente: elaboración propia

5.3 Flujos de información e indicadores

Gobierno Corporativo. - Para el correcto funcionamiento del modelo de gestión tecnológica es necesario que existan flujos de información, los mismos que van interactuando

entre todos los componentes del modelo proporcionando dinámica entre los módulos que integran el modelo propuesto en este estudio.

La activación del modelo de gestión tecnológica inicia con el requerimiento de acatamiento de las directrices emitidas por el Consejo de Aseguramiento de la Calidad de la Educación Superior a las Instituciones de Educación Superior, y el cumplimiento del Modelo de Evaluación Externa de Universidades y Escuelas Politécnicas.

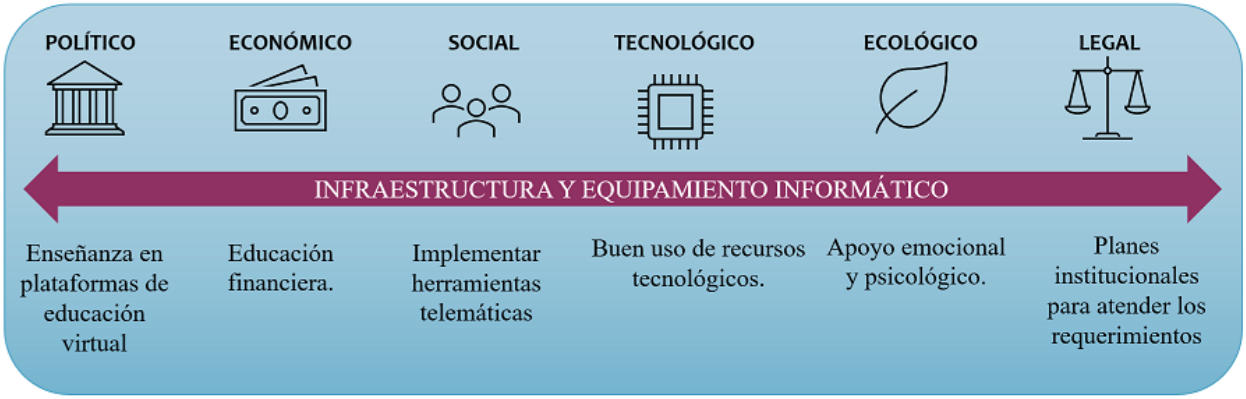
El cumplimiento del Modelo de Evaluación Externa de Universidades y Escuelas Politécnicas está organizado de la siguiente manera: Función, Componente, Dimensión, y Estándar. Para el desarrollo de los indicadores relacionados con tecnología de la información se ha tomado en cuenta el estándar 16 de infraestructura y equipamiento informático, el cual solicita que la institución cuente con una plataforma informática disponible y accesible a la comunidad universitaria para la gestión de los procesos académicos y administrativos. El organismo de control valora el cumplimiento de este hito con la verificación técnica y los formularios estandarizados, lo cual se constituye como un indicador de cumplimiento.

Por consiguiente, el estándar 16 es el primer flujo de información con el cual se inicia el proceso de gestión de riesgos en el grupo correspondiente a Gobierno Corporativo, el resultado de esta gestión de riesgos se convierte en material introductorio para el segundo grupo denominado Gobierno empresarial de la información y tecnología.

Gobierno empresarial de la información y tecnología. – Este grupo está conformado por la gestión estratégica y el sistema de gobierno de tecnologías de la información, donde el flujo de información se encuentra relacionado con la infraestructura y equipo tecnológico tomado en cuenta para realizar el análisis PESTEL, el cual permitirá a las IES descubrir los factores que

puedan perjudicar la evolución de la institución y cuáles afectaciones puede tener en el futuro con relación al giro del negocio. Lo mencionado anteriormente se explica de forma más general en la figura 29.

Figura 29. Resumen de análisis PESTEL



Fuente: elaboración propia

El flujo de información de infraestructura y equipamiento informático también es el insumo de la planeación estratégica.

En esta etapa, como producto para la gestión se generan la táctica y los objetivos estratégicos, los cuales son procesados en el sistema de gobierno de tecnologías de la información. La aplicación de este sistema se ve reflejada en el ámbito de seguridad de la información, siendo esta la encargada de generar el indicador de cumplimiento de continuidad y seguridad.

En última instancia, el indicador de cumplimiento de seguridad y continuidad establecido en el área de seguridad de la información se adhiere al módulo de gestión estratégica, donde aporta a la construcción del indicador de gestión estratégica, espacio en el que a su vez fluye

hasta el grupo de gobierno corporativo donde finalmente es registrado en las actividades de monitoreo.

Capítulo VI. Conclusiones y recomendaciones

6.1 Conclusiones

Gracias a la adopción de un modelo de gestión tecnológica que garantice la fiabilidad y seguridad de repositorios digitales de información de instituciones de educación superior se concluye lo siguiente:

Herramienta de gestión. - Las instituciones de educación superior que adopten el modelo de gestión tecnológica que garantice la fiabilidad y seguridad de repositorios digitales de información de instituciones de educación superior contarán con una herramienta que permita monitorizar el desarrollo de proyectos tecnológicos y contar con una visión clara del retorno de inversión, con lo relacionado a la transformación digital de su institución.

Gobierno. – El concepto de ambiente de control (control interno), en las instituciones se ha transformado en gobierno a partir de la adopción de una cultura de riesgos, ya que actualmente ya no se habla solo de gobierno corporativo. Las instituciones deben tener mayor énfasis en temas relacionados con gobierno corporativo, gobierno de datos, gobierno de tecnologías de información, gobierno de seguridad de la información, gobierno de continuidad del negocio y un nuevo concepto de gobierno de riesgos.

Dirigir y controlar el entorno tecnológico de una IES. - La aplicación de este modelo de gestión de tecnologías de información integrado al área tecnológica permitirá que el órgano colegiado de una Institución de Educación Superior esté en capacidad de dirigir y controlar todo el ámbito relacionado con las tecnologías de información y comunicaciones, generando beneficios a la Institución educativa.

Cumplimiento normativo. - Una de las características del trabajo basado en un marco de desenvolvimiento de función del gobierno corporativo de tecnologías de la información en conjunto con el gobierno corporativo institucional, es que las inspecciones solicitadas por el ente de control se encuentren constantemente monitoreadas de acuerdo con el proceso de mejora continua que están inmersos.

6.2 Recomendaciones

Para un correcto funcionamiento del modelo de gestión tecnológica que garantice la fiabilidad y seguridad de repositorios digitales de información de instituciones de educación superior se recomienda lo siguiente:

Socialización. – Los directivos institucionales deben preparar las estrategias necesarias que involucren talleres de socialización con todos los integrantes de la IES, especialmente en las áreas estratégicas, tecnológicas y seguridad de la información, quienes están en la obligación de aportar para el cumplimiento de los objetivos estratégicos institucionales.

Decisión. - La institución debe contar con la decisión política del Consejo Superior o el Cuerpo Colegiado encargado de realizar dichas funciones dentro de una IES, para generar mecanismos de implementación, como por ejemplo la creación de equipos multidisciplinarios que estén involucrados en la supervisión y ejecución de los objetivos estratégicos que involucren el modelo propuesto.

Equipo de Trabajo. – La conformación del equipo de trabajo debe estar orientada a formar un equipo multidisciplinario compuesto por los responsables en las diferentes áreas o

dueños de los procesos de auditoría interna, seguridad de la información, planificación, y tecnología, quienes colaborarán en función del alineamiento institucional.

Bibliografía

AEC. (s.f.). *COSO.* Gestión de Riesgos : https://www.aec.es/web/guest/centro-conocimiento/coso

Agencia EFE. (2019). *Proyecto de ley de protección de datos en Ecuador es presentado por Mintel.* Seguridad: https://www.elcomercio.com/actualidad/seguridad/proyecto-ley-proteccion-datos-ecuador.html

Angulo, S. (2020). *El Banco Central proyecta que la economía ecuatoriana caerá 8,9 % en 2020 y crecerá 3,1 % en 2021.* Economía: https://www.expreso.ec/actualidad/economia/banco-central-proyecta-economia-ecuatoriana-decrecera-8-9-2020-crecera-3-1-2021-94517.html

Asamblea Nacional. (2018). Ley Orgánica de Educación Superior . Quito, Ecuador.

Asamblea Nacional Constituyente de Ecuador. (2008). Constitución de la República del Ecuador. Quito, Ecuador.

Banco Central del Ecuador. (2020). *La economía ecuatoriana se recuperará 3,1 % en 2021.* https://www.bce.fin.ec/index.php/boletines-de-prensa-archivo/item/1394-la-economia-ecuatoriana-se-recuperara-3-1-en-2021

Ceupe Magazine. (s.f.). *Enfoque holístico en las TIC.* Tecnología: https://www.ceupe.com/blog/enfoque-holistico-en-las-tic.html

Charan, L., & Bossidy, R. (2003). *El arte de la ejecución en los negocios.* Mc. Graw Hill.

COBIT. (2018). *Introducción y metodología.* ISACA. https://issuu.com/sistemas_epuentes/docs/cobit-2019-framework-introduction-and-methodology_

COBIT Diseño. (2019). *Guía de Diseño COBIT.* https://pdfcoffee.com/cobit-2019-design-guideresspa0719pdf-3-pdf-free.html

Consejo de Aseguramiento de la Calidad de la Educación Superior [Caces]. (2019). *Modelo de evaluación externa de universidades y escuelas politécnicas.* https://www.caces.gob.ec/wp-content/uploads/downloads/2019/12/3.-Modelo_Eval_UEP_2019_compressed.pdf

Consejo de Aseguramiento de la Calidad de la Educación Superior [Caces]. (s.f.). *Evaluación externa con fines de acreditación de universidades y escuelas politécnicas.* https://www.caces.gob.ec/institucional/

COSO. (2021). *Welcome to COSO.* https://www.coso.org/Pages/default.aspx

Díaz, B., Bonilla, E., Kleeberg, F., & Noriega, M. (2020). *Mejora continua de los procesos. Herramientas y técnicas.* Lima: Fondo Editorial Universidad de Lima.

Hernández, J. (s.f.). *COBIT, una metodología que genera valor en las empresas.* Universidad Piloto de Colombia. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4677/00004999.pdf?isAllowed=y&sequence=1

Instituto de Auditores Internos de Colombia. (s.f.). *Programa de Certificado de Control Interno COSO.* https://www.iiacolombia.com/seminariostalleres2.php?id=2021-04-13%2014:40:01

Instituto Nacional de Estadística y Censos [INEC]. (2021). *Home.* https://www.ecuadorencifras.gob.ec/

Instituto Nacional de Estadística y Censos [INEC]. (2021). *Tecnologías de la Información y Comunicación, 2020.* INEC. https://www.ecuadorencifras.gob.ec/documentos/web-

inec/Estadisticas_Sociales/TIC/2020/202012_Principales_resultados_Multiproposito_TIC.pdf

Instituto Provincial de Administración Pública de Mendoza. (s.f.). *TIC: Tecnologías de la información y la comunicación.* https://www.mendoza.gov.ar/gobierno/wp-content/uploads/sites/19/2018/09/m4.-Resumen-TIC.pdf

Interpolados. (2016). *Cobit 5: un marco de negocio para el gobierno y la gestión de las TI de la empresa.* Ingeniería y servicios IT: https://interpolados.wordpress.com/2016/08/30/cobit-5-un-marco-de-negocio-para-el-gobierno-y-la-gestion-de-las-ti-de-la-empresa/

Lugo, J. (2015). *Gestión por procesos e indicadores de gestión.* https://es.slideshare.net/juanlugomarin/jl-curso-gestin-por-procesos-e-indicadores-de-gestion

Ministerio de Ambiente del Ecuador. (2017). *Estrategia nacional de educación ambiental para el desarrollo sostenible 2017-2030.* https://www.ambiente.gob.ec/wp-content/uploads/downloads/2018/07/ENEA-ESTRATEGIA.pdf

Naciones Unidas. (2018). *Objetivo 9: Construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación.* https://www.un.org/sustainabledevelopment/es/infrastructure/

Observatorio Regional de Planificación para el Desarrollo de América Latina y el Caribe. (2017). *Plan Nacional del Buen Vivir 2013-2017 de Ecuador.* https://observatorioplanificacion.cepal.org/es/planes/plan-nacional-del-buen-vivir-2013-2017-de-ecuador

Organización Panamericana de la Salud [OPS]. (2020). *La OMS caracteriza a COVID-19 como una pandemia.* https://www.paho.org/es/noticias/11-3-2020-oms-caracteriza-covid-19-como-pandemia

Ortega, O., & Calderón-Salazar, J. (2014). Una Mirada a la Propiedad Intelectual en las Instituciones de Educación Superior de Guayaquil. *Revista Ciencia Unemi*, 88-98. https://www.redalyc.org/pdf/5826/582663858009.pdf

Parada, P. (2013). *Análisis PESTEL, una herramienta de estrategia empresarial de estudio del entorno.* http://www.pascualparada.com/analisis-pestel-una-herramienta-de-estudio-del-entorno/

Pérez, M. (2018). *Qué es el análisis PESTEL.* https://www.zonaeconomica.com/que-es-el-analisis-pestel

Pichincha Comunicaciones. (2019). *Proyecto de Ley de Protección de Datos llegó a la Asamblea Nacional.* Nacionales: https://www.pichinchacomunicaciones.com.ec/proyecto-de-ley-de-proteccion-de-datos-llego-a-la-asamblea-nacional/

Puentes, E. (s.f.). *Capítulo 1 Introducción.* https://issuu.com/sistemas_epuentes/docs/cobit-2019-framework-introduction-and-methodology_/s/10674164

Rivadeneira, L., & Pinedo, V. (2018). *Modelo de gobierno de Tecnología de la Información, basado en gestión del riesgo y seguridad de la información para las Universidades Públicas: caso de estudio Universidad de la Guajira.* Fundación Universitaria del Norte. https://manglar.uninorte.edu.co/bitstream/handle/10584/8330/133663.pdf?sequence=1&isAllowed=y

Romero, A. (2004). *Dirección y planificación estratégicas en las empresas y organizaciones.* Madrid: Díaz de Santos, S.A.

Salah, J. (2017). *Modelo de Gobierno y Gestión de TI basado en la estrategia de Gestión del Riesgo para la Secretaría de Educación de Magdalena Caso de estudio: macroproceso Gestión de la Cobertura.* Fundación Universidad del Norte. http://manglar.uninorte.edu.co/bitstream/handle/10584/8079/131482.pdf?sequence=1&isAllowed=y

Salvador, A. (2016). *COSO: gestión de riesgos.* https://fraudeinterno.wordpress.com/2016/02/19/coso-gestion-de-riesgos/

Secretaría de Educación Pública [SEP]. (s.f.). *Instituciones de Educación Superior.* https://www.gob.mx/sep/acciones-y-programas/instituciones-de-educacion-superior

SGSI. (2017). *Ciberseguridad y seguridad de la información ¿es lo mismo?* https://www.pmg-ssi.com/2017/06/ciberseguridad-seguridad-de-la-informacion/

Superintendencia de compañías, valores y seguros. (2013). Resolución No. SCVS-INC-DNCDN-2020-0013. Quito, Ecuador.

Systems Audit and Control Association [ISACA]. (2020). *COBIT Focus Area: Information Security.* Schaumburg: ISACA.

Tecon. (s.f.). *La Seguridad de la Información.* https://www.tecon.es/la-seguridad-de-la-informacion/

UDG virtual. (s.f.). *Análisis PESTEL.* http://biblioteca.udgvirtual.udg.mx/jspui/bitstream/123456789/2973/1/An%c3%a1lisis%20PESTEL.PDF

World Compliance Association. (2021). *Acerca del Compliance.* https://www.worldcomplianceassociation.com/que-es-compliance.php