RESUMEN – TRABAJO DE GRADO

AUTORES	Yan Carlo Angarita Sanguino
FACULTAD	Facultad de Ingeniería
PLAN DE ESTUDIOS	Maestría de Gobierno de TI
DIRECTOR	PhD. Torcoroma Velázquez Pérez
CODIRECTOR	Msc. Claudia Yamile Gómez Llanez
TÍTULO DE LA TESIS	Modelo de privacidad de la información con enfoque en gestión del conocimiento para los consultorios jurídicos de las instituciones de educación superior de Norte de Santander.
TITULO EN INGLES	Information privacy model with a focus on knowledge management for the legal offices of higher education institutions in Norte de Santander.

RESUMEN
(70 palabras)

Los consultorios jurídicos de las Instituciones de Educación Superior de Norte de Santander atienden usuarios con diversos asuntos legales, requiriendo compartir información relevante. Esta información debe ser protegida, garantizando su privacidad y uso exclusivo para el propósito específico. Este proyecto busca desarrollar un modelo de privacidad de la información, enfocado en la gestión del conocimiento, mediante un diagnóstico inicial, el desarrollo del modelo y su respectiva validación.

RESUMEN EN INGLES

The legal clinics of the Higher Education Institutions of Norte de Santander serve users with various legal matters, requiring the sharing of relevant information. This information must be protected, ensuring its privacy and exclusive use for the specific purpose. This project aims to develop an information privacy model, focused on knowledge management, through an initial diagnosis, model development, and validation.

PALABRAS CLAVES	Privacidad de la Información, Gestión de Conocimiento, Consultorios Jurídicos de las Instituciones de Educación Superior.
PALABRAS CLAVES EN INGLES	Information Privacy, Knowledge Management, Legal Offices of Higher Education Institutions.

CARACTERÍSTICAS

PÁGINAS: 128	PLANOS:	ILUSTRACIONES:	CD-ROM:

Modelo de Privacidad de la Información con Enfoque en Gestión del Conocimiento para los Consultorios Jurídicos de las Instituciones de Educación Superior de Norte de Santander.

Yan Carlo Angarita Sanguino

Facultad de ingeniería, Universidad Francisco de Paula Santander Ocaña

Maestría en Gobierno de TI

PhD. Torcoroma Velázquez Pérez

Msc. Claudia Yamile Gomez

20 de agosto de 2024

Índice

Capítulo 1. Modelo de Privacidad de la Información con Enfoque en Gestión del Conocimiento para los Consultorios Jurídicos de las Instituciones de Educación Superior de Norte de Santander. 10

1.1 Planteamiento del problema 10

1.2 Formulación del problema 13

1.3 Objetivos 14

1.3.1 Objetivo General 14

1.3.2 Objetivos Específicos. 14

1.4 Justificación 15

1.5 Delimitaciones 19

1.5.1 Delimitación geográfica. 19

1.5.2 Delimitación temporal. 19

1.5.3 Delimitación conceptual. 19

1.5.4 Delimitación operativa. 19

Capítulo 2. Marco referencial 20

2.1 Marco histórico 20

2.2 Marco conceptual 21

2.2.1 Consultorios jurídicos. 21

2.2.2 Principios generales de los consultorios jurídicos. 22

2.2.3 Servicios de los Consultorios Jurídicos. 25

2.2.4 Base de datos. 26

2.2.5 Calidad del dato. 26

2.2.6 Confidencialidad. 26

2.2.7 Dato Personal. 26

2.2.8 Dato público. 26

2.2.9 Dato semiprivado. 27

2.2.10 Dato sensible. 27

2.2.11 Derecho de los niños y adolescentes. 27

2.2.12 Encargado del tratamiento. 27

2.2.13 Información digital. 28

2.2.14 Responsable del tratamiento. 28

2.2.15 Titular. 28

2.2.16 Tratamiento. 28

2.2.17 Tratamiento de datos personales. 28

2.2.18 Gestión de conocimiento. 28

2.2.19 Gobierno de TI. 29

2.3 Marco contextual 30

2.4 Marco teórico 31

2.5 Marco legal 32

Capítulo 3. Diseño metodológico 34

3.1 Tipo de investigación 34

3.2 Seguimiento metodológico del proyecto 36

3.3 Población 37

3.4 Muestra 37

3.5 Técnicas de recolección de la información 37

3.6 Análisis de la información 37

Capítulo 4. Resultados 39

4.1 Diagnostico del estado actual de privacidad de la información y la gestión del conocimiento en los consultorios jurídicos de las instituciones de educación superior de Norte de Santander. 39

4.1.1 Componente de procesos 38

4.1.2 Componente de estructuras organizativas 61

4.1.3 Componente de flujos e información 62

4.1.4 Componente de personas, habilidades y competencia 63

4.1.5 Componente de políticas y procedimientos 64

4.1.6 Componente de cultura, ética y comportamiento 65

4.1.7 Componente de servicios, infraestructura y aplicaciones 66

4.1.8 Normativa 67

4.2 Estructura del modelo de privacidad de la información con enfoque en gestión del conocimiento para los consultorios jurídicos de las instituciones de educación superior de Norte de Santander. 68

4.2.1 Modelo de privacidad de la información con enfoque en gestión del conocimiento para los consultorios jurídicos de las instituciones de educación superior. 70

4.2.1.1. Reconocimiento de la organización. 72

4.2.1.2. Diagnóstico de privacidad de la información. 73

4.2.1.3. Socialización de resultados. 75

4.2.1.4 Implementación de prácticas de gobierno y gestión. 77

4.2.1.5 Mejora continua. 80

4.3 Validación del modelo propuesto de privacidad de la información en un consultorio jurídico en una institución de educación superior de Norte de Santander. 82

4.3.1 Selección de expertos. 82

4.3.2 Evaluación del modelo. 87

4.3.3 Validación del modelo. 89

Conclusiones 91

Recomendaciones 94

Referencias 95

Apéndice 99

Lista de Tablas

Tabla 1.*Modelo Metodológico.* 36

Tabla 2.*Evaluación de prácticas de gobierno.* 38

Tabla 3.*Fuentes de argumentación del experto vs Grado de influencia de las fuentes.* 83

Tabla 4.*Determinación del coeficiente del experto.* 84

Tabla 5.*Rangos para definición de coeficiente de competencia.* 86

Tabla 6.*Perfiles de los expertos.* 86

Tabla 7.*Resultados de frecuencia absoluta*..... 87

Tabla 8.*Resultados de frecuencia relativa.* 88

Tabla 9.*Resultados de frecuencia relativa acumulada.* 89

Lista de Figuras

Figura 1.*Matriz metas empresariales a metas de alineamiento.* 34

Figura 2.*Matriz objetivos de gobierno y gestión con metas de alineamiento.*..... 35

Figura 3.*Entrada calculo y salida del factor.* 36

Figura 4.*Niveles de capacidad de los procesos.* 38

Figura 5.*Comparación de niveles de capacidad de la meta de alineamiento – AP012.* 53

Figura 6.*Comparación de niveles de capacidad de la meta de alineamiento – AP013.* 54

Figura 7.*Comparación de niveles de capacidad de la meta de alineamiento – BAI08.* 56

Figura 8.*Comparación de niveles de capacidad de la meta de alineamiento – DSS05.* 57

Figura 9.*Comparación de niveles de capacidad de la meta de alineamiento – MEA03.* 59

Figura 10.*Componentes del sistema de gobierno.* 61

Figura 11.*Modelo de privacidad de la información con enfoque en gestión del conocimiento par**a** los consultorios jurídicos de las instituciones de educación superior..* 71

Figura 12.*Fases del modelo de privacidad de la información con enfoque en gestión del conocimiento para los consultorios jurídicos de las instituciones de educación superior*. 72

Figura 13.*Perfil de expertos.*..... 82

Introducción

El proyecto de investigación tiene como finalidad la creación de un modelo de privacidad de la información con enfoque en gestión del conocimiento para los consultorios jurídicos de las instituciones de educación superior de Norte de Santander que ayude al cumplimiento de la normativa que rige el tratamiento de datos personales por parte de organizaciones públicas o privadas que se establece por la Ley 1581 del 2012, la protección de la información y de los datos que establece La Ley 1273 del 2009 y vigilancia por parte de la superintendencia de industria y comercio en su papel de supervisora aplicando las sanciones correspondientes en los casos que no se valide el cumplimiento de la norma.

Los consultorios jurídicos de las instituciones de educación superior son seleccionados para desarrollar el modelo de privacidad de la información por ser un escenario donde gracias a todos los servicios ofrecidos a la comunidad y a su respectivo funcionamiento que es regido por la Ley 2113 del 2021, se obtiene acceso a mucha información por parte de los usuarios que en caso de no hacer un buen tratamiento de datos personales, se puede afectar con la exposición de datos sensibles para el usuario y en consecuencia el incumplimiento de la norma.

En el primer capítulo se identifica la problemática, los objetivos a realizar, la justificación para la realización del proyecto y las delimitaciones encontradas en el proceso. En el segundo capítulo se encuentra el marco referencial que consta de un marco histórico con los antecedentes, el marco conceptual, el marco contextual, el marco teórico y el marco legal; todo relacionado al modelo de privacidad de la información, gestión del conocimiento, tratamiento de los datos y al

ejercicio desarrollado en los consultorios jurídicos de las instituciones de educación superior de Norte de Santander.

En el tercer capítulo se describe la metodología implementada, el seguimiento metodológico, la población, la muestra, las actividades a realizar para crear los instrumentos de recolección de información y los posibles tipos de análisis de los datos. En el cuarto capítulo se describe el diagnóstico realizado en los consultorios jurídicos, el desarrollo del modelo de privacidad de la información y el proceso de validación del modelo.

Capítulo 1. Modelo de Privacidad de la Información con Enfoque en Gestión del Conocimiento para los Consultorios Jurídicos de las Instituciones de Educación Superior de Norte de Santander.

1.1 Planteamiento del problema

En las instituciones de educación superior que ofrecen el programa de Derecho dentro de su plan de estudios de pregrado, se debe cumplir con la práctica de consultorio jurídico que se define como un "*escenario de aprendizaje práctico en el cual los estudiantes adquieren conocimientos y desarrollan competencias, habilidades y valores éticos para el ejercicio de la profesión de abogado, prestando el servicio obligatorio y gratuito de asistencia jurídica a la población*" (Ley 2113, 2021). Todo el proceso se encuentra reglamentado por la Ley 2113 del 2021 donde se identifica un aspecto muy importante en el Artículo 3 - Punto 10; "*la Confidencialidad, con lo que ningún miembro del consultorio jurídico podrá revelar o utilizar la información suministrada por quienes solicitan la prestación de los servicios, a menos que hayan recibido del solicitante autorización escrita para ellos, o que tengan necesidad de hacer revelaciones para evitar la comisión de un delito"* (Ley 2113 - 2021, art 3).

Con esta característica de la confidencialidad, los consultorios jurídicos también deben ejercer todo lo relacionado a la Ley Estatutaria 1581 por la cual se dictan disposiciones generales para la protección de datos personales. "*Esta ley busca proteger los datos personales registrados en cualquier base de datos y reglamenta también las operaciones que sobre ellos se pueden realizar como son la recolección, almacenamiento, uso, circulación o supresión por parte de*

entidades de naturaleza pública y privada. Esta ley busca salvaguardar los derechos de los ciudadanos consagrados en los artículos 15 y 20 de la constitución política de política de Colombia y el derecho fundamental al hábeas data" (Ley 1581 del 2012).

Otra característica que viene definida constitucionalmente es el derecho a la intimidad conocido como habeas data, donde se declaran que todos los datos de una persona que hacen referencia a su entorno privado y familiar se vuelven impenetrables y nadie puede acceder a ellos. Toda esta legislación hace necesario que las organizaciones públicas y privadas tengan en cuenta el tema de tratamiento de datos y su respectiva reglamentación (Espitia Ruíz, J. J. 2016).

El Ministerios de las TIC promueve en el contexto del tratamiento de los datos personales, la disponibilidad de la información, la integridad y su respectiva confidencialidad a través de su modelo de seguridad y privacidad de la información que mediante la implementación de un proceso de gestión de riesgo se garantice la privacidad de los datos dando como resultado un alto nivel de confianza entre las partes interesadas (Ministerio de las Tecnología y las Comunicaciones, 2016).

En el proceso no se identifican antecedentes de modelos de privacidad de la información en los consultorios jurídicos de las instituciones de educación superior, pero si se encuentran antecedentes relacionados al tratamiento de datos personales como el "Modelo de Gobierno de Tratamiento de la Información para la Empresa Colombiana en la globalización en la prospectiva del desarrollo organizacional" donde se resalta la necesidad del adecuado tratamiento de la

información dentro de las empresas y como se debe tener conciencia para cumplir los requisitos legales y generar valor agregado a la organización (Camargo Barbosa, J. A. ,2018).

También en el "Diagnóstico y Planeación del Modelo de Seguridad y Privacidad de la información en el Hospital San José de Ortega" se ve la importancia del avance para conseguir que los datos personales sensibles se aseguren con el fin de evitar que sea conocida o modificada por personas no autorizadas; logrando todo esto con el buen tratamiento de la información (Triana Acevedo, H. R.).

El tratamiento de los datos dentro de los consultorios jurídicos es muy importante pues se puede tener acceso a datos sensibles por medio de algunos convenios, por ejemplo:

• Programa de Asistencia Legal a Personas con Necesidad de Protección Internacional y Víctima del Conflicto Armado (ALPOSD) a través del cual se da a la población con necesidad de protección internacional y a víctimas de desplazamiento acceso a recursos legales (Red Valor Compartido, 2020).

• Víctimas del conflicto armado en el posconflicto luego de la firma de los Acuerdos de Paz entre el Estado colombiano y las Fuerzas Armadas Revolucionarias de Colombia – Ejército del Pueblo (FARC-EP). El convenio promueve que los estudiantes de los consultorios jurídicos se vinculen al Sistema Autónomo de Asesoría y Defensa Gratuita (SAAD), como medio para una atención a víctimas del conflicto con escasos recursos (Romero Rodríguez, 2021).

Con estos convenios se tiene acceso a información que puede ser utilizada para otros fines en países como Colombia que ha tenido conflictos armados y el tema de la violencia siempre está vigente, muertes de líderes sociales, persecuciones y desplazamientos son casos que se ven a diario. Otro aspecto importante es el cumplimiento de la parte reglamentaria y la legislación colombiana donde se considera infracción a la protección de datos personales cuando se recogen y se tratan datos sin la respectiva autorización, utilización de los datos del usuario para un fin diferente al autorizado entre las más usuales (Asuntos Legales, 2021), por lo que es evidente que en los consultorios jurídicos de las instituciones de educación superior se garantice el cumplimiento de la ley de protección de datos cuando se solicita la información para el respectivo diligenciamiento y ejecución del proceso, evitando a futuro posibles sanciones por parte de la Superintendencia de Industria y Comercio (SIC) en su rol de autoridad nacional de protección de datos personales.

1.2 Formulación del problema

¿Cuáles serían los elementos que integrarían un modelo de privacidad con enfoque en gestión del conocimiento que permita mejorar el tratamiento de los datos personales de los ciudadanos en los consultorios jurídicos de las instituciones de educación superior de Norte de Santander?

1.3 Objetivos

1.3.1 Objetivo General.

Diseñar un modelo de privacidad de la información con enfoque en gestión del conocimiento para los consultorios jurídicos de las instituciones de educación superior de Norte de Santander.

1.3.2 Objetivos Específicos.

Diagnosticar el estado actual de privacidad de la información y de la gestión de conocimiento en los consultorios jurídicos de las instituciones de educación superior de Norte de Santander.

Estructurar el modelo de privacidad de la información con enfoque en gestión del conocimiento para los consultorios jurídicos de las instituciones de educación superior de Norte de Santander.

Validar el modelo propuesto de privacidad de la información con enfoque en gestión del conocimiento en los consultorios jurídicos en una institución de educación superior de Norte de Santander.

1.4 Justificación

En los consultorios jurídicos de las instituciones de educación superior se maneja todo tipo de información según cada caso, desde demandas, derechos de petición, acción de tutela entre otras; que sin importar el contexto de cada situación se debe velar por un buen tratamiento de datos personales. Hay algunos casos que, a través de los convenios nombrados anteriormente, se maneja información más sensible que no solo afecta el buen nombre de las personas; por el contrario, expondría su integridad como se ve en el tema de asesinatos de líderes sociales en Colombia donde se estima que en el 2016 fueron asesinados 166 líderes sociales, mientras que esta cifra fue de 185 para 2017 (Garavito, C. A. R., & Ángel, 2018).

La defensoría del pueblo señaló a través de un informe que entre los años 2016 y 2020 se reconocieron 4.281 conductas que afectaron a líderes sociales, entre estas se identifican 3.184 amenazas, 31 desplazamientos forzados, 753 homicidios, 26 detenciones arbitrarias, 193 atentados, 13 secuestros y 13 desapariciones forzadas. Además, fueron víctimas de "todo tipo de hechos que afectaron sus derechos a la vida, seguridad, integridad personal e integridad", añadió el documento. (DW, 2021).

Con todo esto se identifica la vulnerabilidad que se vive en Colombia por parte del conflicto armado y lo delicado del manejo de la información y la responsabilidad de los consultorios jurídicos de las instituciones de educación superior frente a la información que se maneja. Por otro lado, La Superintendencia de Industria y Comercio (SIC) identifica que durante

el año 2020 se recibieron 16.237 quejas (un promedio mensual de 1.353) donde el 11% se recibieron por eventuales incumplimientos de la Ley Estatutaria 1581 de 2021 (Ley general de protección de datos), en donde la queja principal fue la "Falta de autorización para recolectar y usar los datos". Además, se vienen publicando las sanciones impuestas a organizaciones en el año 2019, 2020 y 2021 donde muestra que están ejecutando los controles para garantizar el cumplimiento de la ley de protección de datos. (SIC, 2021).

También se evidencia que en el año 2020 las quejas por protección de datos subieron un 27% comparado con el año 2019, con lo que emitió 76 sanciones e identificó que dentro de las causas más relevantes de las quejas están, la no solicitud de la autorización para el tratamiento de los datos y la no conservación de la copia de la misma autorización, no mantener la información bajo condiciones de seguridad, no tramitar las consultas y reclamos de los usuarios y no informar la finalidad del uso de la información; en conclusión el no cumplimiento a todo lo referente al tratamiento y protección de datos personales.(SIC, 2020)

En Norte de Santander se encuentran consultorios jurídicos como la Universidad Francisco de Paula Santander sede Ocaña, Universidad Simón Bolívar sede Cúcuta y la Universidad Libre entre otros; estos consultorios jurídicos por estar en la Zona del Catatumbo, que es conocida por una inestabilidad social, violencia, proliferación y fortalecimiento de actores armados ilegales, aumento de cultivos ilícitos y demás representaciones de violencia (Miranda, F. C., & Rodríguez, F. G. O, 2020) hacen que la privacidad de la información de los usuarios sea

sensible resaltando que en el departamento no existe personal dentro de los consultorios que apliquen estándares o buenas prácticas de gobierno de TI. Con todas estas características planteadas, el proceso de tratamientos de datos personales se debe apoyar bajo un marco de trabajo que ayude la implementación de un gobierno de TI, que teniendo en cuenta los procesos de los consultorios jurídicos de las instituciones de educación superior, se puedan integrar estándares, directrices, regulaciones y mejores prácticas.

Con todas estas características planteadas, el proceso de tratamientos de datos personales se debe apoyar bajo un marco de trabajo que ayude la implementación de un gobierno de TI, que teniendo en cuenta los procesos de los consultorios jurídicos de las instituciones de educación superior, se puedan integrar estándares, directrices, regulaciones y mejores prácticas. La implementación del Gobierno de TI en este contexto es crucial para asegurar que los consultorios jurídicos manejen la información de manera segura y eficiente, optimizando recursos, protegiendo datos sensibles y garantizando el cumplimiento normativo. Además, permite una mejor gestión del conocimiento y facilita la adaptabilidad e innovación tecnológica en un entorno de constante cambio y alta sensibilidad.

El resultado que se quiere obtener es un modelo de privacidad de la información que ayude al cumplimiento de la normativa de tratamiento y protección de datos personales contrarrestando todos los problemas mencionados anteriormente. Se busca que el modelo de privacidad de la información se pueda implementar de forma genérica en los consultorios

jurídicos de las instituciones de educación superior de Norte de Santander que funcionan con forme a la Ley 2112 del 2021 y hacen que estos espacios de proyección social de las universidades funcionen de una forma semejante. Es indiferente si el funcionamiento de los consultorios jurídicos se hace netamente presencial y de forma física o si ya se han implementado herramientas tecnológicas para la gestión y almacenamiento de la información; pues en todos los casos se debe cumplir con los requisitos mínimos de la normativa para su correcto cumplimiento.

1.5 Delimitaciones

1.5.1 Delimitación geográfica.

La propuesta de investigación sobre el modelo de privacidad de la información se llevará a cabo en los consultorios jurídicos de las instituciones de educación superior de Norte de Santander.

1.5.2 Delimitación temporal.

La ejecución de las actividades necesarias para el desarrollo de la presente propuesta de investigación tendrá una duración estimada de un (1) año a partir de su aprobación.

1.5.3 Delimitación conceptual.

En el desarrollo de la propuesta de investigación se estudiarán conceptos relacionados con el gobierno y Gestión de Tecnologías de la Información y sus diferentes elementos vistos desde el marco de referencia COBIT 2019. Además, se tendrá en cuenta la legislación que trata con protección de datos personales como la Ley 1581 del 2012, la Ley 1223 del 2009, referente a la protección de información y de los datos y la Ley 2113 del 2021 por medio de la cual se rigen los consultorios jurídicos de las instituciones de educación superior. Por último, están los conceptos de privacidad de la información y gestión de conocimiento.

1.5.4 Delimitación operativa.

Por la zona donde se desarrolla la propuesta de investigación, es frecuente que se presenten problemas de orden público lo cual puede impedir la operación normal de los consultorios y puede impedir la realización de la investigación en estas zonas. De igual manera debido a los diferentes grupos al margen de la ley que serían población de dichos consultorios la información que se maneja es bastante sensible, lo cual podría restringir su disponibilidad.

Capítulo 2. Marco referencial

2.1 Marco histórico

El tema de privacidad de la información siempre ha estado presente dentro de las normas de la sociedad como derechos básicos, como se identifica en la Constitución Colombiana de 1991, en el artículo 15 donde cita "*Todas las personas tienen derecho a su intimidad personal y familiar y a su bien nombre" seguido de "En la recolección, tratamiento y circulación de datos se respetarán la liberta y demás garantías consagradas en la Constitución*" (Constitución Política de Colombia, 1991).

A nivel de Latinoamérica los países siempre han trabajado por cumplir con el nivel adecuado en los temas de protección de datos pues se considera muy importante garantizar el cumplimiento de las normas mínimas. (Remolina, 2010). Países como Argentina con la Ley 25326, Uruguay con la Ley 18331, México con la Ley Federal de Protección de Datos y Perú con la Ley 29733 (Valbuena, 2014) demuestran el avance que se ha logrado en la región. En Colombia se emitió en el año 2012 la "Ley 1581 de 2012" por la cual se dictan disposiciones generales para la protección de datos personales para lo cual se deben garantizar el cumplimiento de unos principios, definición de tipos de datos y tratamiento de datos personales y responsables de su resguardo (Ley 1581 del 2012).

Otro evento importante en Colombia es el Modelo de Seguridad y Privacidad de la Información (MSPI) que emitió el Ministerio de las Tecnologías y las Comunicaciones (MINTIC) en el año 2016. "*El cual se encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la*

Administración del Riesgo y el Diseño Controles en entidades Públicas siendo actualizado periódicamente con las normas técnicas y legislación de la ley de protección de datos personales, transparencia y acceso a la información pública entre otras" (Modelo de Seguridad y Privacidad de la Información, MINTIC, 2016).

Al mismo tiempo el parlamento europeo y el Consejo de la Unión Europea el Reglamento General de protección de Datos (RGPD) hizo referencia al debido tratamiento de datos de las personas y a su libre distribución. En España, la Ley Orgánica de Protección de Datos Personales reemplazo en diciembre del 2018 (LOPD).

Con la obligación por parte de todas las organizaciones que manejan datos personales de sus usuarios, deben garantizar el cumplimiento de la legislación cumpliendo con el tratamiento de los datos personales y todas las características que esto conlleva. Esta situación incluye a los consultorios jurídicos de las instituciones de educación superior que bajo la ley 2113 de 2021 reglamentan su funcionamiento (Ley 2113 - 2021).

2.2 Marco conceptual

2.2.1 Consultorios jurídicos.

Como la investigación se realizará para los consultorios jurídicos es importante entender el concepto, entendiendo por consultorio jurídico de una institución de educación superior *"un escenario de aprendizaje práctico donde los estudiantes del programa de Derecho, bajo la coordinación del personal administrativo y docentes que apoyen el proceso académico, desarrollen competencias y valores éticos para el ejercicio de la profesión, ofreciendo servicios*

obligatorios y gratuitos de asuntos jurídicos a la población de escasos recursos establecido en la presente ley" (Ley 2113, 2021)

2.2.2 Principios generales de los consultorios jurídicos.

- **Educación jurídica práctica**.

"El Consultorio Jurídico garantiza procesos de aprendizaje a partir del acercamiento de los estudiantes a las personas en condición de vulnerabilidad, la sociedad, las necesidades jurídicas que enfrentan y los contextos en que se desarrollan, al igual que fomenta el desarrollo de estrategias y de acciones de defensa de sus derechos dentro de estándares de innovación, calidad y actualidad, colaborando con la administración de justicia y asegurando el cumplimiento del derecho de acceso a la justicia" (Ley 2113, 2021)

- **Autonomía Universitaria.**

"Sin perjuicio de las disposiciones establecidas en el contenido de esta ley, se reconoce la autonomía de las instituciones de educación superior, las cuales cuentan con las competencias para regular todos los aspectos relativos al funcionamiento, administración y reglamento de los consultorios jurídicos, así como la correspondencia entre estos aspectos y el contenido de sus Proyectos Educativos Institucionales y Proyectos Educativos de Programa" (Ley 2113, 2021)

- **Formación Integral**.

"El Consultorio Jurídico constituye un escenario idóneo para la formación académica, profesional, técnica, humana, social y ética del abogado, permitiendo a los estudiantes de Derecho adquirir, mediante experiencias propias del ejercicio de la profesión, los saberes y habilidades necesarias y esperados para el ejercicio de la abogacía" (Ley 2113, 2021)

- **Interés general**.

"El Consultorio Jurídico busca la defensa del interés general, su armonización con los intereses particulares y con los fines del Estado Social de Derecho, propendiendo por la justicia y la equidad en la sociedad" (Ley 2113, 2021)

- **Función social**.

"El Consultorio Jurídico orienta su acción a la defensa de derechos de sujetos de especial protección constitucional y personas naturales que carezcan de medios económicos para contratar los servicios de un profesional en Derecho, o en general personas o grupos que, por sus circunstancias especiales, se encuentren en situación de vulnerabilidad o indefensión, en los términos establecidos en la presente ley" (Ley 2113, 2021)

- **Progresividad**.

"Las prácticas de consultorio jurídico se llevan a cabo de manera progresiva con el programa de la Institución de Educación Superior de acuerdo con su naturaleza, modalidad y metodología" (Ley 2113, 2021)

- **Gratuidad**.

"El Consultorio Jurídico presta servicios jurídicos gratuitos en favor de las personas beneficiadas que se definen en esta ley. Los gastos necesarios para el impulso procesal y las costas judiciales en los trámites que apliquen serán asumidos por el usuario y en ningún caso los asumirá el estudiante" (Ley 2113, 2021)

- **Inclusión**.

"El Consultorio Jurídico garantiza los ajustes razonables necesarios para asegurar que los estudiantes, docentes y las personas beneficiarias de sus servicios puedan tener acceso y participar activamente en ellos, en igualdad de condiciones. Así mismo, fomenta en los estudiantes una perspectiva de igualdad, respeto por la diversidad e inclusión" (Ley 2113, 2021)

- **Accesibilidad**.

"El Consultorio Jurídico asegura a todos los estudiantes, docentes y usuarios el acceso en igualdad de condiciones al entorno físico, la información y las comunicaciones relacionadas con la prestación de sus servicios, y establece parámetros que les permitan acceder a servicios no presenciales. En relación con los usuarios de la administración de justicia, facilitan, en la medida de sus posibilidades y conforme a lo que se determine en los reglamentos de las instituciones de educación superior, que los sujetos procesales puedan acceder en sus sedes a las actuaciones virtuales" (Ley 2113, 2021)

- **Confidencialidad**.

"Los miembros del Consultorio Jurídico no podrán revelar o utilizar la información suministrada por quienes solicitan la prestación de sus servicios, a menos que hayan recibido del solicitante autorización escrita para ello, o que tengan necesidad de hacer revelaciones para evitar la comisión de un delito" (Ley 2113, 2021)

- **Calidad**.

"Cada Universidad fijará los estándares que garanticen la calidad y eficiencia en la prestación del servicio en el correspondiente consultorio jurídico y centro de conciliación" (Ley 2113, 2021)

2.2.3 Servicios de los Consultorios Jurídicos.

Los Consultorios Jurídicos de las IES "prestarán servicios de asesoría jurídica, representación judicial y extrajudicial a toda la comunidad beneficiaria, adelantamiento de actuaciones administrativas e interposición de recursos en cualquier oficina administrativa. Además, se prestarán servicios de procesos de conciliación en contextos de equidad, mecanismos de justicia y restauración, medicación y temas de interés público", así como todos los demás servicios que tengan relación y permitan el cumplimiento de lo establecido en la ley 2113 del 2021.

Los servicios de asesoría jurídica ofrecidos por los Consultorios Jurídicos podrán prestarse en entidades privadas o públicas, notarias, organismos internacionales, despachos judiciales, cajas de compensación familiar y centros de conciliación. Se atenderán a personas de especial protección constitucional, a personas naturales que sean beneficiarios, y en general a todos aquellos, que, por sus circunstancias especiales, se definan en situación de vulnerabilidad o indefensión. Los demás servicios se prestarán a personas con dificultades económicas para contratar los servicios de un profesional y la información que se suministre no podrá darse a conocer a ningún tercero, entidades u organismos oficiales. Solo se podrán dar resúmenes numéricos, con lo que se garantice que no se puede identificar ningún usuario individualmente y usar los datos con otra finalidad.

2.2.4 Base de datos.

"Conjunto organizado de Datos Personales que sean objeto de tratamiento. Incluye archivos físicos y electrónicos" (Ley 1581 de 2012)

2.2.5 Calidad del dato.

"El dato personal sometido a tratamiento deberá ser veraz, completo, exacto, actualizado, comprobable y comprensible. Cuando se esté en poder de datos personales parciales, incompletos, fraccionados o que induzcan a error" (Ley 1581 de 2012)

2.2.6 Confidencialidad.

"Elemento de seguridad de la información que permite establecer quienes y bajo qué circunstancias se puede acceder a la misma" (Ley 1581 de 2012)

2.2.7 Dato Personal.

"Cualquier información vinculada o que pueda asociarse a una o a varias personas naturales determinadas o determinables. Debe entonces entenderse el dato personal como una información relacionada con una persona natural (persona individualmente considerada)" (Ley 1581 de 2012)

2.2.8 Dato público.

"Los datos públicos son aquellos relacionados al estado civil de las personas, a la profesión u oficio que ejercen y su participación como comerciante o de servidor público. Este tipo de dato puede encontrase en registros y documentos públicos o sentencias judiciales que no estén en reserva" (Ley 1581 de 2012)

2.2.9 Dato semiprivado.

"Es aquella información que no es de naturaleza íntima, reservada ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como es el caso de los datos financieros, crediticios o actividades comerciales" (Ley 1581 de 2012)

2.2.10 Dato sensible.

"Aquel dato que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos" (Ley 1581 de 2012)

2.2.11 Derecho de los niños y adolescentes.

"En el Tratamiento se asegurará el respeto a los derechos prevalentes de los niños y adolescentes. Sólo podrán tratarse aquellos datos que sean de naturaleza pública" (Ley 1581 de 2012)

2.2.12 Encargado del tratamiento.

"Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento" (Ley 1581 de 2012)

2.2.13 Información digital.

"Toda aquella información que es almacenada o transmitida por medios electrónicos y digitales como el correo electrónico u otros sistemas de información" (Ley 1581 de 2012)

2.2.14 Responsable del tratamiento.

"Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos" (Ley 1581 de 2012)

2.2.15 Titular

"Persona natural cuyos datos personales son objeto de Tratamiento" (Ley 1581 de 2012)

2.2.16 Tratamiento

"Es cualquier operación o conjunto de operaciones sobre Datos Personales que realice los encargados del tratamiento, tales como recolección, almacenamiento, uso, circulación o supresión" (Ley 1581 de 2012)

2.2.17 Tratamiento de datos personales.

"Son las operaciones que se ejercen sobre los datos personales, recolección, uso, almacenamiento, transporte o supresión" (Ley 1581 de 2012)

2.2.18 Gestión de conocimiento.

"Coordinación y control de todo el activo intelectual que tiene una organización, dirigido a aportar un valor adicional a cada proceso, adaptándose a todos los cambios que pueden existir en el contexto, sobre la base de la cultura organizacional, el liderazgo y la cooperación mutua. Todo este proceso se fundamenta en poder convertir el conocimiento tácito en explícito" (Montejo, Y. C., & Sousa, H. P. ,2021).

2.2.19 Gobierno de TI.

"Procesos generales para dirigir y controlar la empresa hacia el logro de sus objetivos añadiendo valor en todas las áreas, buscando en cada avance un balance entre el riesgo y el retorno sobre las TI y sus procesos. El gobierno de TI institucionaliza las buenas prácticas para garantizar que TI en la empresa están alineados a los objetivos del negocio. Ayuda a la empresa en aprovechar su información, maximizando los beneficios, capitalizando las oportunidades y obteniendo ventajas competitivas" (Periñán, I. L. M., & Villegas, G. U, 2011).

2.3 Marco contextual

El proyecto se desarrollará en Norte de Santander que es uno de los 32 departamentos de Colombia, ubicado en la zona nororiental del país sobre la frontera con Venezuela. El departamento contiene la región del Catatumbo la cual hace parte de los territorios focalizados PDET (Programa de desarrollo con enfoque territorial), pues siempre ha tenido inconvenientes de inseguridad y presencia de grupos al margen de la ley.

En el departamento de Norte de Santander se encuentran 6 consultorios jurídicos de instituciones de educación superior, donde 5 de ellos se encuentran en la ciudad de San José de Cúcuta donde se atienden los usuarios que necesitan los servicios de los consultorios; añadiendo que, debido a la situación de Venezuela, la migración de personas del vecino país ha producido una mayor inseguridad en la región y nuevas modalidades de atención a través del programa de ALPOSD.

El estado colombiano a través de leyes establece los lineamientos para el cumplimiento de todo lo relacionado a un buen tratamiento de datos personales en cualquier entidad que maneje los datos de sus usuarios y existen entidades a cargo del control y vigilancia como lo es en este caso la Superintendencia de Industria y Comercio (SIC) garantizando el derecho constitucional que tienen todas las personas a conocer, actualizar, rectificar, suprimir y revocar la autorización respecto a las informaciones que hayan recogido sobre ellas las entidades públicas y privadas.

2.4 Marco teórico

El proyecto se realiza con base a regulaciones o buenas prácticas en gobierno de TI y el buen tratamiento de datos personales. En lo que se refiere a las teorías y buenas prácticas de Modelos de Gobierno se puede buscar en el Marco de Negocio para el Gobierno y la Gestión de TI de la Empresa donde se fundamentan 5 principios relacionados. Estos principios son el de satisfacer las necesidades de las partes interesadas, cubrir la empresa en general, aplicar un marco que sea de referencia integrado, propender un enfoque holístico y mantener separado el gobierno de la gestión (Camargo Barbosa, J. A. ,2018).

La ley 1581 de 2012 para el tratamiento de datos personales, crea un escenario que obliga a las instituciones públicas y privadas a cumplir con ciertos lineamientos con respecto a la privacidad de la información y principios que son necesarios tener presentes en el proceso de tratamiento de los datos. El principio de legalidad, el principio de la finalidad en la cual el titular debe ser informado del uso final de sus datos, el principio de libertad que se refiere a que los datos solo se pueden usar bajo consentimiento del titular, el principio de veracidad y calidad que garantiza que los datos veraces, completos y comprobables. El titular de la información tiene derecho a saber quién posee sus datos bajo el principio de transparencia, el principio de acceso y circulación donde solo las personas autorizadas pueden hacer uso de los datos del titular. Los 2 principios adicionales son lo de seguridad donde se debe garantizar la seguridad de los datos del titular y el principio de confidencialidad con el cual los datos deben ser privados, confidenciales y resguardados aun después de ya no tener relación con el titular. (Ley 1581 de 2012)

2.5 Marco legal

"Constitución Política de Colombia de 1991. Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar" (Constitución Política de Colombia)

"Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos. Esta ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como recolección, almacenamiento, uso, circulación o supresión por parte de entidades de naturaleza pública y privada" (Ley 1581 de 2012)

"Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones" (Ley 1273 de 2009)

"Decreto 1377 de 2013. Se reglamenta parcialmente la Ley 1581 de 2012, facilitando la implementación y el cumplimiento de la Ley 1581 de 2012, reglamentando aspectos particulares relacionados con la autorización del titular de la información para el tratamiento de sus datos personales, además consagra políticas de tratamiento de los responsables y encargados" (Decreto 1377 de 2013)

"Ley 1266 de 2008. Contempla las disposiciones generales en relación con el derecho de habeas data y se regula el manejo de la información contenida en bases de datos personales, en

especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones" (Ley 1266 de 2008)

"Ley 2113 de 2021. Por la cual se regula el funcionamiento de los consultorios jurídicos de las instituciones de educación superior" (Ley 2113 de 2021)

Capítulo 3. Diseño metodológico

3.1 Tipo de investigación

Esta investigación se abordará bajo un enfoque cuantitativo donde las hipótesis propuestas se pueden validar con el análisis de la información obtenida a través de técnicas de recolección de datos. (Ackerman & Com, 2013), considerando el paradigma positivista, y un alcance descriptivo, que gracias al proceso se pueden obtener diagnósticos respecto a un tema en particular (Ackerman & Com, 2013), usando un método de proyecto factible.

La investigación se apoyará en el método etnográfico (Miguélez, M. M. 2005) para conocer mejor el funcionamiento de los consultorios jurídicos de las instituciones de educación superior identificando sus principales características y aspectos relevantes que puedan afectar la investigación, la recolección de los datos e implementación del modelo que dé como resultado de todo el proceso.

En el contexto de la investigación cuantitativa, se decidió utilizar la encuesta como el principal método para adquirir datos de los consultorios jurídicos de las instituciones de educación superior en Norte de Santander. Al enfocarse en la medición y el cálculo, la encuesta facilitó la obtención de información cuantificable sobre varias variables relevantes para el estudio. A través de este procedimiento, se obtuvieron datos esenciales acerca del estado actual de la integración del gobierno y gestión de TI.

La siguiente fase del análisis se enfocó en emplear los datos recopilados para extraer conclusiones significativas. La autenticidad y fiabilidad de estos datos fueron aspectos esenciales durante todo el proceso de investigación. La autenticidad garantizó que las mediciones y datos obtenidos fueran representativos y pertinentes para los objetivos del estudio, mientras que la fiabilidad aseguró la coherencia y precisión de los resultados a lo largo de la encuesta, proporcionando confianza en la veracidad de la información analizada. Por ende, la aplicación de estos principios en la investigación cuantitativa proporcionó un sólido marco para un análisis riguroso y significativo de la situación de los consultorios jurídicos de las IES en lo referente a la privacidad de la información y gestión del conocimiento.

Además, al interpretar con precisión los datos recolectados mediante la aplicación de las directrices COBIT 2019, se logró una comprensión profunda de la dinámica operativa actual de personas, grupos y sistemas. Al centrarse en hechos concretos y ofrecer interpretaciones precisas respaldadas por estas directrices reconocidas, la investigación descriptiva fue fundamental para una comprensión más completa de la situación y la identificación de áreas clave para mejorar la gestión del conocimiento y la privacidad de la información en los consultorios jurídicos de las IES.

3.2 Seguimiento metodológico del proyecto

Para el cumplimiento del objetivo general es importante el desarrollo de cada objetivo específico, por tanto, se describe en una tabla el seguimiento de cada objetivo, con sus actividades y el indicador por cada una de ellas (ver Tabla 1).

Tabla 1.*Modelo Metodológico.*

OBJETIVOS DE LA INVESTIGACIÓN	ACTIVIDADES POR OBJETIVO	INDICADOR POR ACTIVIDAD
Diagnosticar el estado actual de privacidad de la información y gestión del conocimiento en los consultorios jurídicos de las instituciones de educación superior de Norte de Santander.	Diseñar los instrumentos de recolección de información necesarios.	Instrumento de recolección de información (Encuesta).
	Aplicar los instrumentos de recolección de la información a la muestra definida.	Información recolectada.
	Analizar los resultados obtenidos de los instrumentos de recolección de información.	Gráfica de análisis estadísticos. Diagnóstico
Estructurar el modelo de privacidad de la información con enfoque en gestión del conocimiento para los consultorios jurídicos de las instituciones de educación superior de Norte de Santander.	Identificar los elementos del modelo.	Elementos del modelo.
	Diseñar el modelo.	Modelo estructurado.
Validar el modelo propuesto de privacidad de la información con enfoque en gestión del conocimiento de un consultorio jurídico de una institución de educación superior de Norte de Santander.	Seleccionar el método de validación.	Método de validación.
	Aplicar el método de validación seleccionado.	Aplicación del método.
	Analizar los resultados obtenidos del método de validación aplicado.	Modelo validado

3.3 Población

En Norte de Santander existen 6 (seis) consultorios jurídicos los cuales se encuentran 5 (cinco) en la ciudad de Cúcuta (Universidad Simón Bolívar, Universidad Francisco de Paula Santander, Universidad de Pamplona, Universidad de Santander y la Universidad Libre) y 1(uno) en el municipio de Ocaña. El proyecto se centra en los consultorios jurídicos ubicados en Norte de Santander con el propósito de poder hacer el proceso de recolección de los datos.

3.4 Muestra

Se tomará el 50% de la población como muestra representativa que equivale a 3 consultorios jurídicos.

3.5 Técnicas de recolección de la información

Como técnica de recolección de información se utilizará las encuestas o cuestionarios, el método de observación (si es necesario) utilizando un guion de preguntas. Para profundizar el conocimiento en los observatorios se contará con el apoyo de las entrevistas.

3.6 Análisis de la información

Por ser investigación de corte cuantitativo para el análisis de la información, se utiliza estadística descriptiva, para lo cual se apoyará con herramientas como SPSS, utilizando Alpha de

Cronbach, análisis de curva ROC entre otras para el análisis de datos. Para las entrevistas si es caso se trabajará con atlas TI para la generación de redes semánticas.

Capítulo 4. Resultados

4.1 Diagnostico del estado actual de privacidad de la información y la gestión del conocimiento en los consultorios jurídicos de las instituciones de educación superior de Norte de Santander.

Primero, se establece una matriz que vincula las metas empresariales con las metas de alineamiento. Se debe dar un puntaje de 10 a las metas empresariales que se consideren importantes dentro de los consultorios jurídicos de las IES (ver Figura 1). Esta evaluación refleja la relevancia de cada meta empresarial en relación con los objetivos estratégicos definidos. Las metas empresariales priorizadas fueron:

- EG02: Gestión de riesgo de negocio.
- EG03: Cumplimiento con las leyes y regulaciones externas.
- EG06: Continuidad y disponibilidad del servicio del negocio.
- EG10: Habilidades, motivación y productividad del personal.
- EG11: Cumplimiento de las políticas internas.
- EG13: Innovación de producto y negocio.

Estas metas seleccionadas indicarán cuáles son las más importantes y alineadas con los objetivos estratégicos de los consultorios jurídicos de las IES.

A continuación, se procede a desarrollar una matriz que vincule las metas empresariales previamente seleccionadas con las metas de alineamiento genéricas de COBIT 2019 (ver Figura 1). Cada una de las metas empresariales seleccionadas recibirá un peso uniforme de 1. A continuación, se empleará una escala de valoración donde se asigna un puntaje de 5 a las metas

consideradas como "Principal" (P) y un puntaje de 1 a las clasificadas como "Secundario" (S), evaluando así la relevancia de cada meta de alineamiento en relación con las metas empresariales. Posteriormente, se realizará una suma de los puntajes asignados a cada meta de alineamiento en función de su alineación con las metas empresariales seleccionadas. Por último, se identificarán las metas de alineamiento que obtengan las puntuaciones más altas en la matriz, lo que indicará cuáles de estas metas están más alineadas y tienen mayor prioridad en el contexto de las metas empresariales seleccionadas (ver Figura 1). Las metas de alineamiento elegidas fueron:

- AG01: Cumplimiento y soporte de I&T para el cumplimiento empresarial con las leyes y regulaciones externas.
- AG02: Gestión de riesgo relacionado con I&T.
- AG07: Seguridad de la información, infraestructura y aplicaciones de procesamiento y privacidad.
- AG11: Cumplimiento de I&T con las políticas internas.
- AG12: Personal competente y motivado con un entendimiento mutuo de la
- tecnología y el negocio.
- AG13: Conocimiento, experiencia e iniciativas para la innovación empresarial.

En relación con las metas empresariales elegidas para los consultorios jurídicos de las IES, tal como se muestra en la Figura 2, se han identificado como prioritarios los objetivos de gobierno y gestión de mayor puntaje y valor que son el resultado de las metas empresariales y metas de alineamiento priorizadas:

APO12.01 Recopilar datos.
APO12.02 Analizar el riesgo.
APO12.03 Mantener un perfil de riesgo.
APO12.04 Articular el riesgo.

APO12.05 Definir un portafolio con acciones de gestión de riesgos.

APO12.06 Responder al riesgo.

APO13.01 Establecer y mantener un sistema de gestión de seguridad de la información (SGSI).

APO13.02 Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad.

APO13.03 Monitorizar y revisar el sistema de gestión de seguridad de la información (SGSI).

BAI08.01 Identificar y clasificar las fuentes de información para el gobierno y la gestión de I&T.

BAI08.02 Organizar y contextualizar la información en conocimiento.

BAI08.03 Utilizar y compartir conocimiento.

BAI08.04 Evaluar y actualizar o retirar la información.

DSS05.01 Proteger contra software malicioso.

DSS05.02 Gestionar la seguridad de la conectividad y de la red.

DSS05.03 Gestionar la seguridad de endpoint.

DSS05.04: Gestionar la identidad del usuario y el acceso lógico.

DSS05.05 Gestionar el acceso físico a los activos de I&T.

DSS05.06: Gestionar documentos sensibles y dispositivos de salida.

DSS05.07 Gestionar las vulnerabilidades y monitorizar la infraestructura para detectar eventos relacionados con la seguridad.

MEA03.01 Identificar los requisitos externos de cumplimiento.

MEA03.02 Optimizar la respuesta a los requisitos externos.

MEA03.03 Confirmar el cumplimiento externo.

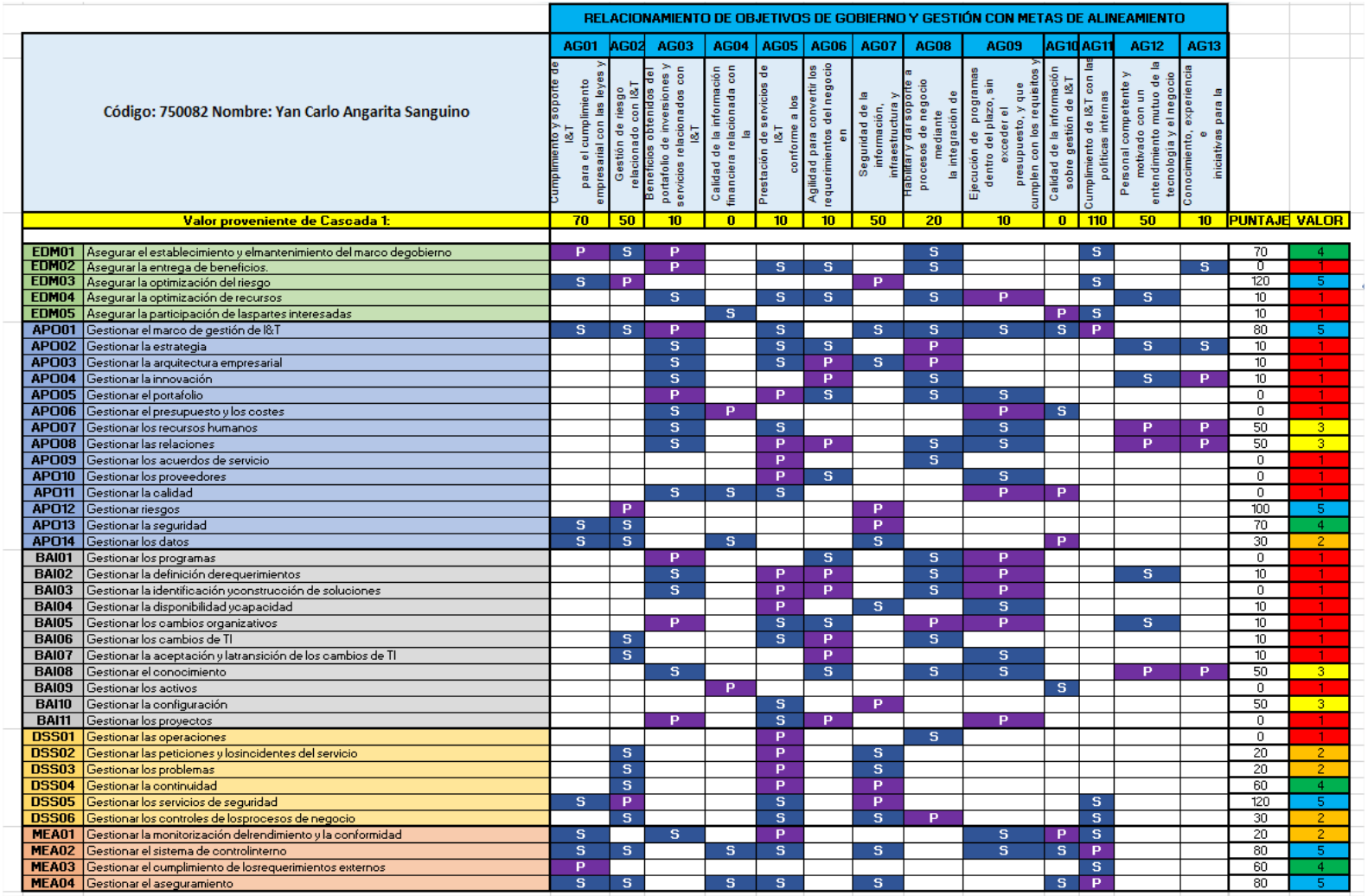
MEA03.04 Obtener aseguramiento de cumplimiento externo.

El puntaje asignado a las metas de alineamiento y la priorización de los objetivos de gobierno y gestión se lleva a cabo siguiendo las pautas establecidas en el diseño de ISACA-COBIT 2019, que es una guía esencial para el diseño de soluciones de gobierno de TI (ver Figura 3).

Figura 1.*Matriz metas empresariales a metas de alineamiento.*

Código: 750082 Nombre: Yan Carlo Angarita Sanguino			RELACIONAMIENTO DE METAS EMPRESARIALES Y METAS DE ALINEAMIENTO													
			EG01	EG02	EG03	EG04	EG05	EG06	EG07	EG08	EG09	EG10	EG11	EG12	EG13	
			Portafolio de productos y servicios competitivos	Gestión de riesgo de negocio	Cumplimiento de leyes y regulaciones externas	Calidad de la información financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio del negocio	Calidad de la información de gestión	Optimización de la funcionalidad de procesos internos del negocio	Optimización de costes de los procesos del negocio	Habilidades, motivación y productividad del personal	Cumplimiento con las políticas internas	Gestión de programas de transformación digital	Innovación de producto y negocio	
Asigne un valor de 10 a cada objetivo de negocio que sea de interés para su organización			0	10	10	0	0	0	0	10	0	10	10	0	0	PUNTAJE
Financiera	AG01	Cumplimiento y soporte de I&T para el cumplimiento empresarial con las leyes y regulaciones externas		S	P								S			70
	AG02	Gestión de riesgo relacionado con I&T		P				S								50
	AG03	Beneficios obtenidos del portafolio de inversiones y servicios relacionados con I&T	S				S			S	S			P		10
	AG04	Calidad de la información financiera relacionada con la tecnología				P			P		P					0
Cliente	AG05	Prestación de servicios de I&T conforme a los requerimientos del negocio	P				S	S		S				S		10
	AG06	Agilidad para convertir los requerimientos del negocio en soluciones operativas	P				S			S				S	S	10
Interna	AG07	Seguridad de la información, infraestructura y aplicaciones de procesamiento y privacidad		P				P								50
	AG08	Habilitar y dar soporte a procesos de negocio mediante la integración de aplicaciones y tecnología	P				P			S		S		P	S	20
	AG09	Ejecución de programas dentro del plazo, sin exceder el presupuesto, y que cumplen con los requisitos y estándares de calidad	P				S			S	S			P	S	10
	AG10	Calidad de la información sobre gestión de I&T				P			P		S					0
	AG11	Cumplimiento de I&T con las políticas internas		S	P								P			110
Aprendizaje y crecimiento	AG12	Personal competente y motivado con un entendimiento mutuo de la tecnología y el negocio					S					P				50
	AG13	Conocimiento, experiencia e iniciativas para la innovación empresarial	P		S									S	P	10

Figura 2.*Matriz objetivos de gobierno y gestión con metas de alineamiento.*



Código: 750082 Nombre: Yan Carlo Angarita Sanguino		RELACIONAMIENTO DE OBJETIVOS DE GOBIERNO Y GESTIÓN CON METAS DE ALINEAMIENTO														
		AG01	AG02	AG03	AG04	AG05	AG06	AG07	AG08	AG09	AG10	AG11	AG12	AG13		
		Cumplimiento y soporte de I&T para el cumplimiento empresarial con las leyes y	Gestión de riesgo relacionado con I&T	Beneficios obtenidos del portafolio de inversiones y servicios relacionados con I&T	Calidad de la información financiera relacionada con la	Prestación de servicios de I&T conforme a los	Agilidad para convertir los requerimientos del negocio en	Seguridad de la información, infraestructura y	Habilitar y dar soporte a procesos de negocio mediante la integración de	Ejecución de programas dentro del plazo, sin exceder el presupuesto, y que cumplen con los requisitos y	Calidad de la información sobre gestión de I&T	Cumplimiento de I&T con las políticas internas	Personal competente y motivado con un entendimiento mutuo de la tecnología y el negocio	Conocimiento, experiencia e iniciativas para la		
Valor proveniente de Cascada 1:		70	50	10	0	10	10	50	20	10	0	110	50	10	PUNTAJE	VALOR
EDM01	Asegurar el establecimiento y elmantenimiento del marco degobierno	P	S	P					S			S			70	4
EDM02	Asegurar la entrega de beneficios.			P		S	S		S					S	0	1
EDM03	Asegurar la optimización del riesgo	S	P					P				S			120	5
EDM04	Asegurar la optimización de recursos			S		S	S		S	P			S		10	1
EDM05	Asegurar la participación de laspartes interesadas				S						P	S			10	1
APO01	Gestionar el marco de gestión de I&T	S	S	P		S		S	S	S	S	P			80	5
APO02	Gestionar la estrategia			S		S	S		P				S	S	10	1
APO03	Gestionar la arquitectura empresarial			S		S	P	S	P						10	1
APO04	Gestionar la innovación			S			P		S				S	P	10	1
APO05	Gestionar el portafolio			P		P	S		S	S					0	1
APO06	Gestionar el presupuesto y los costes			S	P					P	S				0	1
APO07	Gestionar los recursos humanos			S		S				S			P	P	50	3
APO08	Gestionar las relaciones			S		P	P		S	S			P	P	50	3
APO09	Gestionar los acuerdos de servicio					P			S						0	1
APO10	Gestionar los proveedores					P	S			S					0	1
APO11	Gestionar la calidad			S	S	S				P	P				0	1
APO12	Gestionar riesgos		P					P							100	5
APO13	Gestionar la seguridad	S	S					P							70	4
APO14	Gestionar los datos	S	S		S			S			P				30	2
BAI01	Gestionar los programas			P			S		S	P					0	1
BAI02	Gestionar la definición derequerimientos			S		P	P		S	P			S		10	1
BAI03	Gestionar la identificación yconstrucción de soluciones			S		P	P		S	P					0	1
BAI04	Gestionar la disponibilidad ycapacidad					P		S		S					10	1
BAI05	Gestionar los cambios organizativos			P		S	S		P	P			S		10	1
BAI06	Gestionar los cambios de TI		S			S	P		S						10	1
BAI07	Gestionar la aceptación y latransición de los cambios de TI		S				P			S					10	1
BAI08	Gestionar el conocimiento			S			S		S	S			P	P	50	3
BAI09	Gestionar los activos				P						S				0	1
BAI10	Gestionar la configuración					S		P							50	3
BAI11	Gestionar los proyectos			P		S	P			P					0	1
DSS01	Gestionar las operaciones					P			S						0	1
DSS02	Gestionar las peticiones y losincidentes del servicio		S			P		S							20	2
DSS03	Gestionar los problemas		S			P		S							20	2
DSS04	Gestionar la continuidad		S			P		P							60	4
DSS05	Gestionar los servicios de seguridad	S	P			S		P				S			120	5
DSS06	Gestionar los controles de losprocesos de negocio		S			S		S	P			S			30	2
MEA01	Gestionar la monitorización delrendimiento y la conformidad	S		S		P				S	P	S			20	2
MEA02	Gestionar el sistema de controlinterno	S	S		S	S		S		S	S	P			80	5
MEA03	Gestionar el cumplimiento de losrequerimientos externos	P										S			60	4
MEA04	Gestionar el aseguramiento	S	S		S	S		S			S	P			80	5

Figura 3.*Entrada calculo y salida del factor.*

Entrada	• Cada una de las trece metas empresariales deben clasificarse entre 1 (nada importante) y 5 (más importante). • Usando las metas empresariales genéricas se determinan las metas más importantes para la empresa. Es aconsejable seleccionar las tres a cinco primeras metas empresariales más importantes; demasiadas metas de alta prioridad producirán unos resultados de la cascada de metas menos significativos. • Se recomienda mantener la suficiente distancia entre los valores.
Cálculo	• La herramienta realiza un doble cálculo de matrices entre (1) las metas empresariales clasificadas y la tabla de asignación entre las metas empresariales y las metas de alineamiento de TI, y (2) el resultado del primer cálculo de matrices y la tabla de asignación entre las metas de alineamiento de TI y los objetivos de gobierno y gestión. • La herramienta realiza una segunda serie de cálculos de matrices de una serie de valores de referencia para el factor de diseño 2 *Metas empresariales*, lo que deriva en un puntaje de referencia para cada objetivo de gobierno/gestión. • La herramienta calcula a continuación la importancia relativa de cada objetivo de gobierno/gestión como una diferencia relativa entre ambos conjuntos de valores, expresado como un porcentaje y redondeado a 5. Este número puede ser positivo o negativo, indicando que un objetivo de gobierno/gestión es más o menos importante a la hora de hacer una comparación con el puntaje de referencia.
Salida	• La sección de Salida de esta hoja contiene la importancia relativa calculada para cada uno de los 40 objetivos de gobierno y gestión de COBIT® 2019. • Los resultados se representan en formato de tabla, como un diagrama de barras y un diagrama de araña.

Con el enfoque puesto en los objetivos de gobierno y gestión, se ha desarrollado un instrumento para evaluar el estado actual de la privacidad de la información y la gestión del conocimiento en los consultorios jurídicos de las instituciones de educación superior del Norte de Santander (ver Anexo 2).

El diseño del instrumento de evaluación y diagnóstico de privacidad de información y gestión del conocimiento se somete a un proceso riguroso de validación llevado a cabo por tres expertos en el campo de Gobierno de TI a los que se les realiza una encuesta para determinar el coeficiente de competencia del experto (ver Anexo 4). Estos profesionales aportaron una perspectiva crítica y especializada, evaluando la relevancia, claridad y coherencia de este.

Además, analizaron la idoneidad del instrumento para capturar la información necesaria para los objetivos de la investigación y para medir con precisión los conceptos pertinentes en el ámbito de la privacidad de la información y gestión del conocimiento en los consultorios jurídicos de las instituciones de educación superior. Gracias a sus valiosas observaciones y recomendaciones, se realizaron ajustes y mejoras significativas en el instrumento, asegurando así su validez y confiabilidad en la recopilación de datos para el estudio. Este proceso de validación demuestra un compromiso con la calidad y precisión en la investigación (ver Anexo 3).

Este instrumento de diagnóstico se ha aplicado en tres consultorios jurídicos de la región, revelando los promedios de resultados de cada práctica de gobierno evaluada. Durante el proceso de aplicación del instrumento, los encuestados han asignado niveles de capacidad (ver Figura 4) a cada actividad relacionada con las prácticas de gobierno, basándose en los criterios y el grado de cumplimiento de dichas actividades.

4.1.1 Componente de procesos

En la siguiente tabla (ver Tabla 2) se detallan los resultados promedios entre los 3 consultorios jurídicos del componente de procesos y las actividades que pertenecen a cada practica de gobierno. Se podrá identificar la práctica de gobierno, las actividades y el promedio de los niveles de capacidad asignados en cada caso.

Figura 4.*Niveles de capacidad de los procesos.*

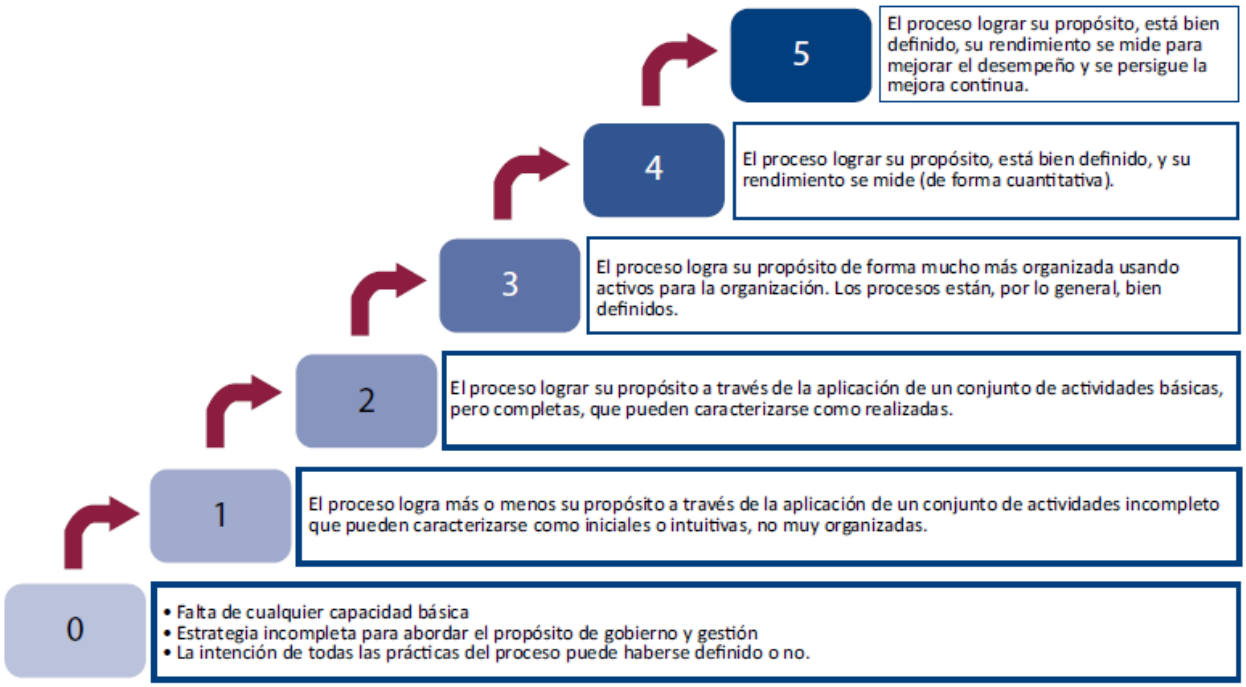


Tabla 2.*Evaluación de prácticas de gobierno.*

PRACTICA GOBIERNO	ACTIVIDAD	PROMEDIO
APO12.01 Recopilar datos	1. Establecer y mantener un método para la recogida, clasificación y análisis de datos relacionados con el riesgo de I&T. 2. Registrar datos relevantes y significativos relacionados con los riesgos de I&T en el entorno operativo interno y externo de la empresa.	0,2

	3. Adoptar o definir una taxonomía de riesgo para las definiciones consistentes de escenarios de riesgo y categorías de impacto y probabilidad. 4. Registrar datos de eventos de riesgo que han causado o podrían causar impacto en el negocio conforme a las categorías de impacto definidas en la taxonomía de riesgo. Capturar datos relevantes de cuestiones, incidentes, problemas e investigaciones. 5. Estudiar y analizar los datos históricos de riesgo de I&T y de pérdidas experimentadas a partir de datos y tendencias externos disponibles, homólogos de la industria a través de logs de eventos de la industria, bases de datos, y acuerdos de la industria, para la publicación común de eventos. 6. Para clases de eventos similares, organizar los datos recopilados y resaltar los factores causantes. Determinar los factores causantes comunes en múltiples eventos. 7. Determinar las condiciones específicas que existieron o estuvieron ausentes cuando tuvieron lugar los eventos de riesgo y la forma en que las condiciones afectaron a la frecuencia del evento y la magnitud de la pérdida. 8. Realizar un análisis periódico de eventos y factores de riesgo para identificar riesgos nuevos o emergentes y para mejorar el entendimiento de los factores de riesgo internos y externos asociados.	
APO12.02 Analizar el riesgo	1. Definir el alcance adecuado de los esfuerzos en análisis de riesgos, considerando todos los factores de riesgo y/o la criticidad de los activos para el negocio. 2. Crear y actualizar regularmente los escenarios de riesgo de I&T; las exposiciones a pérdidas relacionadas con I&T; y los escenarios relacionados con el riesgo reputacional, incluidos escenarios compuestos de tipos de amenazas y eventos en cascada y/o coincidentes. Desarrollar previsiones para actividades de control específicas y capacidades de detección.	0

	3. Estimar la frecuencia (o probabilidad) y la magnitud de la pérdida o ganancia asociada con escenarios de riesgos de I&T. Tener en cuenta todos los factores de riesgo aplicables y evaluar controles operativos conocidos. 4. Comparar el riesgo actual (exposición a pérdidas de I&T) con el apetito al riesgo y la tolerancia de riesgo aceptable. Identificar el riesgo inaceptable o elevado. 5. Proponer respuestas al riesgo para riesgos que excedan el apetito al riesgo y los niveles de tolerancia. 6. Especificar los requisitos de alto nivel para los proyectos o programas que implementarán las respuestas a los riesgos seleccionadas. Identificar los requisitos y expectativas para los controles clave adecuados a fin de proporcionar respuestas de mitigación de riesgos. 7. Validar el análisis de riesgo y los resultados del análisis de impacto del negocio (BIA) antes de usarlos en la toma de decisiones. Confirmar que el análisis se corresponde con los requisitos empresariales y comprobar que los sesgos de las estimaciones se calibraron y analizaron de forma adecuada. 8. Analizar el coste/beneficio de las posibles opciones de respuesta al riesgo, como evitar, reducir/mitigar, transferir/compartir y aceptar y explotar/ aprovechar. Confirmar la respuesta óptima al riesgo.	
APO12.03 Mantener un perfil de riesgo	1. Hacer un inventario de los procesos de negocio y documentar su dependencia con los procesos de gestión de servicios de I&T y los recursos de infraestructura de TI. Identificar el personal de apoyo, aplicaciones, infraestructura, instalaciones, registros manuales críticos, contratistas, proveedores, y terceros. 2. Determinar y acordar qué servicios de I&T y recursos de infraestructura de TI son esenciales para sostener el funcionamiento de los procesos de negocio. Analizar las	0,5

	dependencias e identificar los eslabones débiles. 3. Agregar los escenarios de riesgos actuales por categoría, línea de negocio y área funcional. 4. Capturar regularmente toda la información del perfil de riesgo y consolidarla en un perfil de riesgo agregado. 5. Capturar información sobre el estado del plan de acción de riesgos para su inclusión en el perfil de riesgo de I&T de la empresa. 6. Con base en todos los datos del perfil de riesgo, definir un conjunto de indicadores de riesgo que permitan una identificación y monitorización rápida del riesgo actual y las tendencias de riesgo. 7. Capturar información sobre eventos de riesgo de I&T que se han materializado para su inclusión en el perfil de riesgo de TI de la empresa.	
APO12.04 Articular el riesgo	1. Informar sobre los resultados del análisis de riesgo a todas las partes interesadas afectadas en términos y formatos útiles para soportar las decisiones empresariales. Siempre que sea posible, incluir las probabilidades y rangos de pérdidas o ganancias, junto con los niveles de confianza, para permitir que la gerencia haga balance del retorno del riesgo. 2. Proporcionar a los responsables de la toma de decisiones la comprensión de los escenarios más probables y peores, exposiciones a pérdidas de I&T y consideraciones significativas de reputación, legales y regulatorias, o cualquier otra categoría de impacto conforme a la taxonomía de riesgos. 3. Informar sobre el perfil de riesgo actual a todas las partes interesadas. Incluir información sobre la eficacia del proceso de gestión de riesgos, eficacia del control, brechas, inconsistencias, redundancias, estado de remediación y sus impactos en el perfil de riesgo. 4. De forma periódica, en áreas con riesgos relativos y capacidades de riesgo similares,	0,3

	identificar oportunidades relacionadas con I&T que permitirían la aceptación de un riesgo mayor y un mayor crecimiento y retorno. 5. Revisar los resultados de las evaluaciones objetivas de terceros y revisiones de auditoría interna y de aseguramiento de la calidad. Incluirlos en el perfil de riesgo. Revisar las brechas identificadas y las exposiciones de pérdidas relacionadas con I&T para determinar la necesidad de un análisis de riesgos adicional.	
APO12.05 Definir un portafolio con acciones de gestión de riesgos	1. Mantener un inventario de las actividades de control que se han implantado para mitigar el riesgo y que permiten que se tomen riesgos alineados con el apetito y la tolerancia al riesgo. Clasificar las actividades de control y asignarlas a escenarios de riesgos de I&T específicos y escenarios de riesgos de I&T agregados. 2. Determinar si cada entidad organizativa monitoriza el riesgo y acepta la responsabilidad de actuar dentro de los niveles de tolerancia individuales y del portafolio. 3. Definir un conjunto de propuestas de proyectos equilibrada diseñada para reducir el riesgo y/o proyectos que permitan oportunidades empresariales estratégicas, con consideración de los costes, beneficios, efecto en el perfil de riesgo actual y en las regulaciones.	0,1
APO12.06 Responder al riesgo	1. Preparar, mantener y probar planes que documenten los pasos específicos que deben darse cuando un evento de riesgo pudiera causar un incidente significativo de desarrollo u operativo con un impacto grave para el negocio. Asegurar que los planes incluyan vías de escalamiento en la empresa. 2. Aplicar el plan de respuesta adecuado para minimizar el impacto cuando ocurren incidentes de riesgo. 3. Clasificar los incidentes y comparar las exposiciones a pérdidas relacionadas con I&T con los umbrales de tolerancia al	0,1

	riesgo. Comunicar los impactos de negocio a los responsables de la toma de decisiones como parte del reporte y actualización del perfil de riesgo. 4. Examinar eventos adversos/pérdidas y oportunidades del pasado no consideradas y determinar las causas raíz. 5. Comunicar la causa raíz, requisitos adicionales de respuestas al riesgo y mejoras del proceso a los responsables de la toma de decisiones correspondientes. Asegurar que la causa, requisitos de respuesta y mejora del proceso se incluyan en los procesos de gobierno del riesgo.	
APO13.01 Establecer y mantener un sistema de gestión de seguridad de la información (SGSI).	1. Definir el alcance y los límites del sistema de gestión de seguridad de la información (SGSI) en términos de las características de la empresa, organización, ubicación, activos y tecnología. Incluir detalles y justificación de las exclusiones del alcance. 2. Definir un SGSI conforme a la política empresarial y el contexto en el que opera la empresa, 3. Alinear el SGSI con el enfoque global de la empresa hacia la gestión de la seguridad. 4. Obtener la autorización de la dirección para implementar y operar o cambiar el SGSI. 5. Preparar y mantener una declaración de aplicabilidad que describa el alcance del SGSI. 6. Definir y comunicar los roles y responsabilidades de la gestión de seguridad de la información. 7. Comunicar la estrategia de SGSI.	0
APO13.02 Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad	1. Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con objetivos estratégicos y la arquitectura empresarial. Asegurar que el plan identifique las prácticas de gestión y las soluciones de seguridad apropiadas y óptimas, con los recursos, responsabilidades y prioridades asociados para la gestión de los riesgos de seguridad de la información identificados.	0,2

	2. Mantener, como parte de la arquitectura de la empresa, un inventario de los componentes de la solución establecida para gestionar los riesgos relacionados con la seguridad. 3. Desarrollar propuestas para implementar el plan de tratamiento de riesgos de seguridad, apoyadas por casos de negocio apropiados que incluyan consideraciones de financiación y asignación de roles y responsabilidades. 4. Proporcionar aportes para el diseño y desarrollo de prácticas y soluciones de gestión, seleccionadas en el plan de tratamiento de riesgos de seguridad de la información. 5. Implementar programas de formación y concienciación sobre seguridad de la información y privacidad. 6. Integrar la planificación, diseño, implementación y monitorización de procedimientos de seguridad de la información y privacidad y otros controles capaces de permitir la prevención, detección rápida de eventos de seguridad y la respuesta a incidentes de seguridad. 7. Definir cómo medir la eficacia de las prácticas de gestión seleccionadas. Especificar cómo deben usarse estas medidas para evaluar la eficacia para producir resultados comparables y reproducibles.	
APO13.03 Monitorizar y revisar el sistema de gestión de seguridad de la información (SGSI)	1. Llevar a cabo revisiones regulares de la eficacia del SGSI. Incluir el cumplimiento de la política y los objetivos del SGSI y revisar las prácticas de seguridad y privacidad. 2. Realizar auditorías de SGSI a intervalos planificados. 3. Realizar periódicamente una revisión de la gestión del SGSI para asegurar que el alcance sigue siendo adecuado y que se identifican mejoras en el proceso del SGSI. 4. Registrar acciones y eventos que podrían tener un impacto en la eficacia o el rendimiento del SGSI.	0

	5. Hacer aportes para el mantenimiento de los planes de seguridad para tener en cuenta los hallazgos de las actividades de monitorización y revisión.	
BAI08.01 Identificar y clasificar las fuentes de información para el gobierno y la gestión de I&T	1. Identificar usuarios con conocimiento potenciales, incluidos dueños de información que tal vez deban contribuir y aprobar el conocimiento. Obtener requisitos de conocimiento y fuentes de información de los usuarios identificados. 2. Considerar los tipos de contenido (procedimientos, procesos, estructuras, conceptos, políticas, reglas, hechos, clasificaciones), artefactos (documentos, registros, vídeo, voz) e información estructurada y no estructurada (expertos, redes sociales, correo electrónico, mensajes de voz, canales RSS (Rich Site Summary)). 3. Clasificar las fuentes de información con base en el esquema de clasificación de contenidos (p. ej. el modelo de arquitectura de la información). Correlacionar las fuentes de información con el esquema de clasificación. 4. Recopilar, cotejar y validar las fuentes de información con base en los criterios de validación de la información (p. ej., comprensión, relevancia, importancia, integridad, precisión, consistencia, confidencialidad, vigencia y confiabilidad).	04
BAI08.02 Organizar y contextualizar la información en conocimiento	1. Identificar atributos compartidos y relacionar sus fuentes de información, con la creación de relaciones entre los conjuntos de información (etiquetado de la información). 2. Crear vistas de conjuntos de datos relacionados, considerando los requisitos organizativos y de las partes interesadas. 3. Idear e implementar un esquema para gestionar el conocimiento no estructurado que no está disponible a través de fuentes formales (p.ej. el conocimiento de expertos). 4. Publicar y hacer que el conocimiento sea accesible a las partes interesadas relevantes, conforme a mecanismos de roles y acceso.	0,3

BAI08.03 Utilizar y compartir conocimiento	1. Establecer expectativas de gestión y demostrar la actitud adecuada en cuanto a la utilidad del conocimiento y la necesidad de compartir el conocimiento relacionado con el gobierno y la gestión de la I&T de la empresa. 2. Identificar usuarios potenciales de conocimiento por medio de la clasificación del conocimiento. 3. Transferir el conocimiento a los usuarios del conocimiento, con base en un análisis de brechas de necesidades y técnicas de aprendizaje efectivas. Crear un entorno, herramientas y artefactos que respalden el intercambio y la transferencia de conocimiento. Asegurar que se cuenta con los controles de acceso adecuados, en línea con la clasificación de conocimiento definida. 4. Medir el uso de las herramientas y elementos de conocimiento y evaluar el impacto en los procesos de gobierno. 5. Mejorar la información y el conocimiento de los procesos de gobierno que muestran brechas de conocimientos.	0,4
BAI08.04 Evaluar y actualizar o retirar la información	1. Definir los controles para la retirada de conocimientos y proceder a su retirada como corresponda. 2. Evaluar la utilidad, relevancia y valor de los elementos del conocimiento. Actualizar la información desactualizada que podría seguir siendo relevante y valiosa para la organización. Identificar la información relacionada que ya no es relevante para los requisitos de conocimiento de la empresa y retirarla o archivarla conforme a la política.	0,5
DSS05.01 Proteger contra software malicioso	1. Instalar y activar herramientas de protección contra software malicioso en todas las instalaciones de procesamiento, con archivos de definición de software malicioso que se actualizan según sea necesario (automática o semiautomáticamente). 2. Filtrar el tráfico de entrada, como el correo electrónico y las descargas, para protegerlo	1,5

	de información no solicitada (p.ej. spyware, correos electrónicos de phishing). 3. Comunicar acerca de concienciación sobre software malicioso y hacer cumplir los procedimientos y responsabilidades de prevención. Impartir formación periódica sobre malware en el uso de correo electrónico e Internet. Formar a los usuarios para que no abran e informen sobre correos electrónicos sospechosos y no instalen software compartido o no aprobado. 4. Distribuir todo el software de protección centralmente (versión y parches) usando una configuración centralizada y la gestión de cambios de TI. 5. Revisar y evaluar la información sobre nuevas amenazas potenciales (p. ej., revisión de los consejos de seguridad de productos y servicios de proveedores) de forma regular.	
DSS05.02 Gestionar la seguridad de la conectividad y de la red	1. Permitir que solo los dispositivos autorizados tengan acceso a la información corporativa y a la red de la empresa. Configurar estos dispositivos para forzar la introducción de contraseña. 2. Implementar mecanismos de filtrado de red, como firewalls y software de detección de intrusos. Hacer cumplir las políticas adecuadas para controlar el tráfico entrante y saliente. 3. Aplicar protocolos de seguridad aprobados a las conexiones de red. 4. Configurar el equipo de red de forma segura. 5. Encriptar la información en tránsito de acuerdo a su clasificación. 6. Establecer y mantener una política para la seguridad de la conectividad con base en las evaluaciones de riesgo y los requisitos del negocio. 7. Establecer mecanismos confiables para apoyar la transmisión y recepción segura de la información. 8. Llevar a cabo pruebas de penetración periódicas para determinar la idoneidad de la protección de la red.	0,9

	9. Llevar a cabo pruebas periódicas a la seguridad del sistema para determinar la idoneidad de la protección del sistema.	
DSS05.03 Gestionar la seguridad de endpoint	1. Configurar los sistemas operativos de forma segura. 2. Implementar mecanismos de bloqueo de dispositivos. 3. Gestionar el acceso y control remotos (p.ej. dispositivos móviles, teletrabajo). 4. Gestionar la configuración de red de forma segura. 5. Implementar el filtrado de tráfico de red en dispositivos de punto final. 6. Proteger la integridad del sistema. 7. Proporcionar protección física a los dispositivos de punto final. 8. Eliminar de forma segura los dispositivos Endpoint. 9. Gestionar el acceso malicioso a través del correo electrónico y los navegadores web. Por ejemplo, bloquear determinados sitios web y desactivar los clics a enlaces para los smartphones. 10. Encriptar la información almacenada de acuerdo a su clasificación.	1,5
DSS05.04: Gestionar la identidad del usuario y el acceso lógico	1. Mantener los derechos de acceso de los usuarios de acuerdo con la función del negocio, los requisitos del proceso y las políticas de seguridad. Alinear la gestión de identidades y derechos de acceso con los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad-de-tener y necesidad-de-conocer. 2. Administrar oportunamente todos los cambios en los derechos de acceso (creación, modificación y eliminación), basándose únicamente en transacciones aprobadas y documentadas que hayan sido autorizadas por personas designadas por la dirección. 3. Segregar, reducir al mínimo necesario y gestionar activamente cuentas de usuario privilegiadas. Asegurar la supervisión de todas las actividades en estas cuentas.	1,9

	4. Identificar de forma unívoca y por roles funcionales todas las actividades de procesamiento de información. Coordinarse con las unidades de negocio para asegurarse de que todos los roles están definidos de manera consistente, incluidos los roles definidos por el propio negocio dentro de las aplicaciones de procesos del negocio. 5. Autenticar todo el acceso a activos de información de acuerdo con el rol del individuo o a las reglas del negocio. Coordinarse con las unidades de negocio que gestionan la autenticación dentro de las aplicaciones utilizadas en los procesos de negocio, con el fin de asegurar que los controles de autenticación hayan sido administrados adecuadamente. 6. Garantizar que todos los usuarios (internos, externos y temporales) y su actividad en los sistemas de TI (aplicación de negocio, infraestructura de TI, operaciones, desarrollo y mantenimiento de sistemas) se puedan identificar de manera unívoca. 7. Mantener un registro de auditoría del acceso a la información dependiendo de su sensibilidad y de los requisitos regulatorios. Llevar a cabo revisiones gerenciales periódicas de todas las cuentas y privilegios relacionados.	
DSS05.05 Gestionar el acceso físico a los activos de I&T	1. Registrar y monitorizar todos los puntos de entrada a las instalaciones de TI. Registrar a todos los visitantes al sitio, incluidos contratistas y proveedores. 2. Asegurar que todo el personal muestra una identificación debidamente autorizada en todo momento. 3. Requerir a los visitantes que estén acompañados en todo momento durante su estancia en las instalaciones. 4. Restringir y monitorizar el acceso a instalaciones sensibles de TI, mediante el establecimiento de restricciones al perímetro, como vallas, paredes y dispositivos de seguridad en puertas interiores y exteriores.	1,5

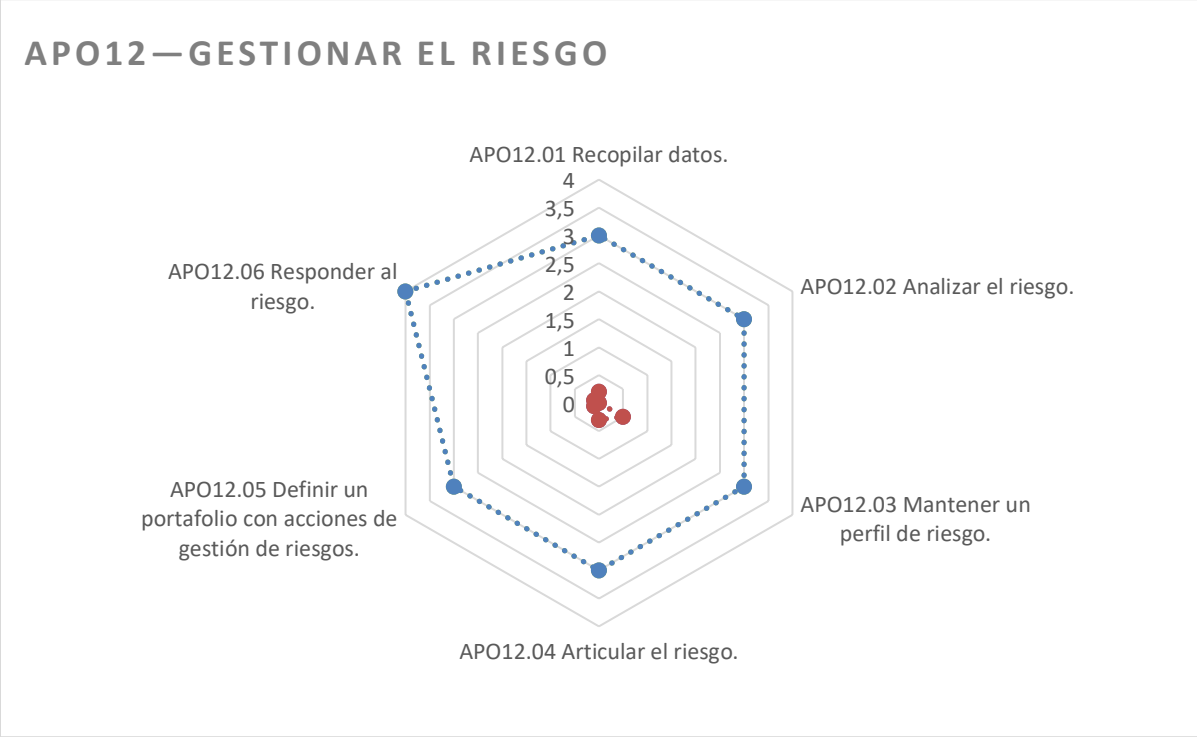
	5. Gestionar solicitudes para permitir el acceso debidamente autorizado a las instalaciones de cómputo. 6. Garantizar que los perfiles de acceso permanezcan actualizados. Basar el acceso a las instalaciones de TI (sala de servidores, edificios, áreas o zonas) en el cargo y las responsabilidades. 7. Realizar formación sobre concienciación de la seguridad de la información física de forma regular.	
DSS05.06: Gestionar documentos sensibles y dispositivos de salida	1. Establecer procedimientos para gobernar la recepción, uso, retiro y desecho de documentos sensibles y dispositivos de salida, dentro y fuera de la empresa. 2. Asegurar que se han establecido controles criptográficos para proteger información sensible almacenada electrónicamente. 3. Asignar privilegios de acceso a documentos sensibles y dispositivos de salida con base en el principio de menor privilegio, manteniendo un equilibrio entre el riesgo y los requisitos del negocio. 4. Establecer un inventario de documentos sensibles y dispositivos de salida y realizar reconciliaciones periódicas. 5. Establecer salvaguardas físicas adecuadas para documentos sensibles.	0,7
DSS05.07 Gestionar las vulnerabilidades y monitorizar la infraestructura para detectar eventos relacionados con la seguridad	1. Usar de forma continua un portafolio de tecnologías, servicios y activos soportados (p. ej., escáneres de vulnerabilidad, fuzzers y sniffers, analizadores de protocolos) para identificar vulnerabilidades de seguridad de la información. 2. Definir y comunicar escenarios de riesgo para que se puedan reconocer con facilidad y se pueda entender su probabilidad e impacto. 3. Revisar regularmente los logs de eventos para detectar posibles incidentes. 4. Garantizar que se creen tickets relativos a incidentes de seguridad de forma oportuna cuando la monitorización identifique posibles incidentes.	0,4

	5. Registrar eventos relacionados con la seguridad y conservar los registros durante el periodo de tiempo apropiado.	
MEA03.01 Identificar los requisitos externos de cumplimiento	1. Asignar la responsabilidad de identificar y supervisar los cambios en los requisitos legales, regulatorios y otros requisitos contractuales externos, relevantes para el uso de recursos de TI y el procesamiento de la información dentro de las operaciones empresariales y de TI. 2. Identificar y evaluar todos los posibles requisitos de cumplimiento y su impacto en las actividades de I&T, en áreas como flujo de datos, privacidad, controles internos, informes financieros, regulaciones específicas de la industria, propiedad intelectual, salud y seguridad en el trabajo. 3. Evaluar el impacto de los requisitos legales y regulatorios relacionados con I&T sobre contratos con terceros relacionados con las operaciones de TI, proveedores de servicio y otros socios comerciales de negocios. 4. Definir las consecuencias del incumplimiento. 5. Obtener asesoría independiente cuando corresponda, sobre los cambios en la legislación, regulaciones y estándares vigentes. 6. Mantener un registro actualizado de todos los requisitos legales, regulatorios y contractuales; de su impacto y las acciones requeridas. 7. Mantener un registro global, armonizado e integrado, de los requisitos de cumplimiento externo para la empresa.	1,2
MEA03.02 Optimizar la respuesta a los requisitos externos	1. Revisar y ajustar continuamente las políticas, principios, estándares, procedimientos y metodologías para que sean eficaces en garantizar el cumplimiento necesario y abordar el riesgo empresarial. Usar expertos internos y externos, cuando sea necesario. 2. Comunicar los requisitos nuevos y modificados a todo el personal relevante.	1,5
MEA03.03 Confirmar el	1. Evaluar regularmente las políticas, estándares, procedimientos y metodologías	1

cumplimiento externo	organizativas en todas las funciones de la empresa, para garantizar el cumplimiento de todos los requisitos legales y regulatorios relevantes relacionados con el procesamiento de la información. 2. Tratar las brechas de cumplimiento en políticas, estándares y procedimientos con la debida oportunidad. 3. Evaluar periódicamente los procesos y actividades del negocio y de TI para asegurar el cumplimiento de los requisitos legales, regulatorios y contractuales vigentes. 4. Revisar regularmente los patrones recurrentes de fallos de cumplimiento y evaluar las lecciones aprendidas. 5. Mejorar las políticas, estándares, procedimientos, metodologías y sus procesos y actividades asociadas con base en la revisión y las lecciones aprendidas.	
MEA03.04 Obtener aseguramiento de cumplimiento externo	1. Obtener confirmación periódica del cumplimiento con las políticas internas por parte de los dueños de los procesos de negocio y de TI y los jefes de unidades. 2. Realizar periódicamente revisiones internas y externas (independientes, cuando sea posible) para evaluar los niveles de cumplimiento. 3. Si se requiere, obtener declaraciones de los proveedores de servicio externos de I&T sobre sus niveles de cumplimiento con las leyes y regulaciones aplicables. 4. Si se requiere, obtener declaraciones de los socios de negocio sobre sus niveles de cumplimiento con leyes y regulaciones aplicables, en la medida en que estén relacionados con las transacciones electrónicas entre empresas. 5. Integrar los informes sobre los requisitos legales, regulatorios y contractuales a nivel global de la empresa, involucrando a todas las unidades de negocio. 6. Supervisar y comunicar los problemas de incumplimiento y, cuando sea necesario, investigar la causa raíz.	1,1

Se generan gráficos utilizando los datos de los niveles de capacidad asignados y promediados para obtener una visualización más detallada de los resultados de la aplicación de los instrumentos en los consultorios jurídicos. Estas gráficas comparan los niveles de capacidad otorgados por los encuestados con el nivel mínimo aceptado para cada actividad.

Figura 5.*Comparación de niveles de capacidad de la meta de alineamiento – AP012.*

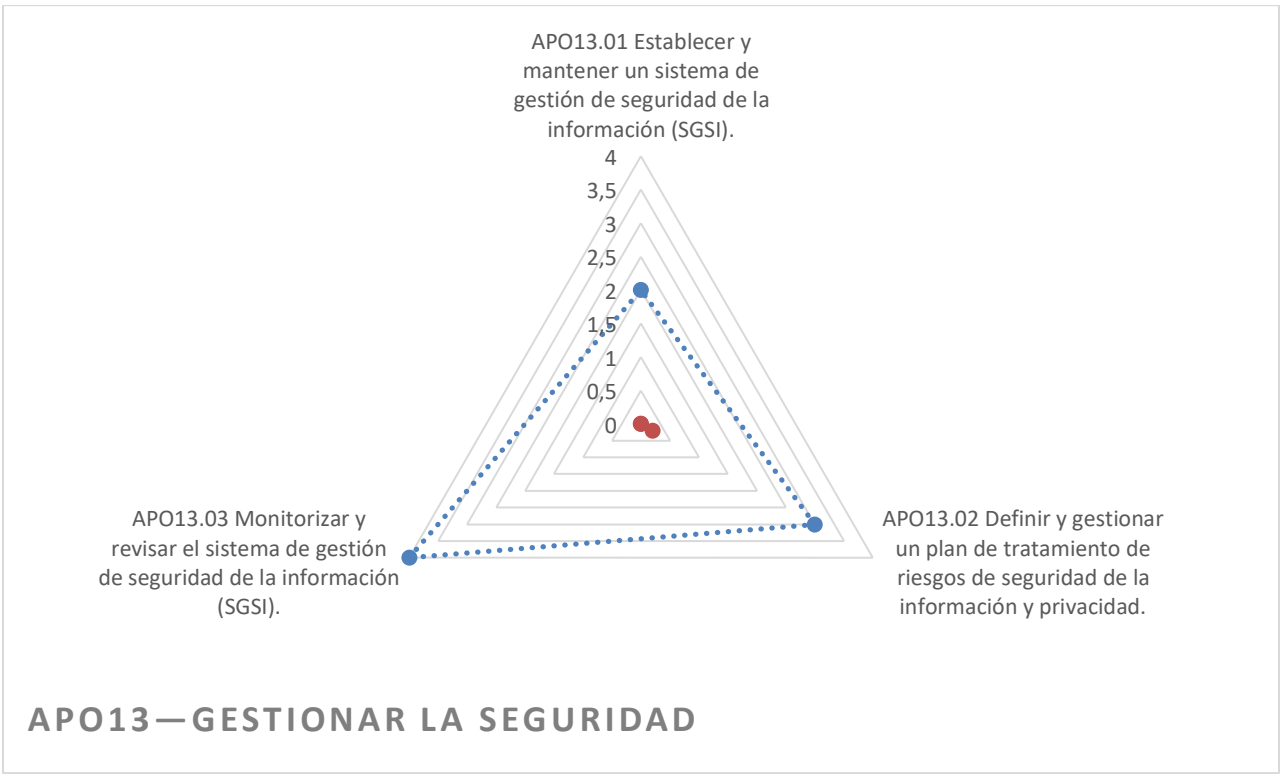


En la primera practica de gobierno evaluada en los consultorios jurídicos de las instituciones de educación superior, se observa una notable falta de atención al objetivo de gestionar el riesgo dentro del marco de trabajo de COBIT 2019 (ver Figura 5). Esta falta de enfoque se manifiesta en la ausencia de actividades clave como la recopilación de información, el análisis de riesgos, la creación de perfiles de riesgo y la articulación de estos riesgos con otras áreas pertinentes.

La falta de recopilación de información impide una comprensión completa de los riesgos a los que se enfrenta la institución, lo que a su vez dificulta la toma de decisiones informadas. Además, sin un análisis exhaustivo de los riesgos, es imposible priorizarlos y asignar recursos de manera eficiente para mitigarlos.

La ausencia de perfiles de riesgo dificulta aún más la identificación de áreas críticas que requieren atención inmediata, lo que puede llevar a una exposición innecesaria a posibles amenazas. Asimismo, la falta de articulación de los riesgos con otras áreas de la institución limita la capacidad de implementar estrategias integrales de gestión de riesgos que aborden los desafíos de manera holística.

Figura 6.*Comparación de niveles de capacidad de la meta de alineamiento – AP013.*

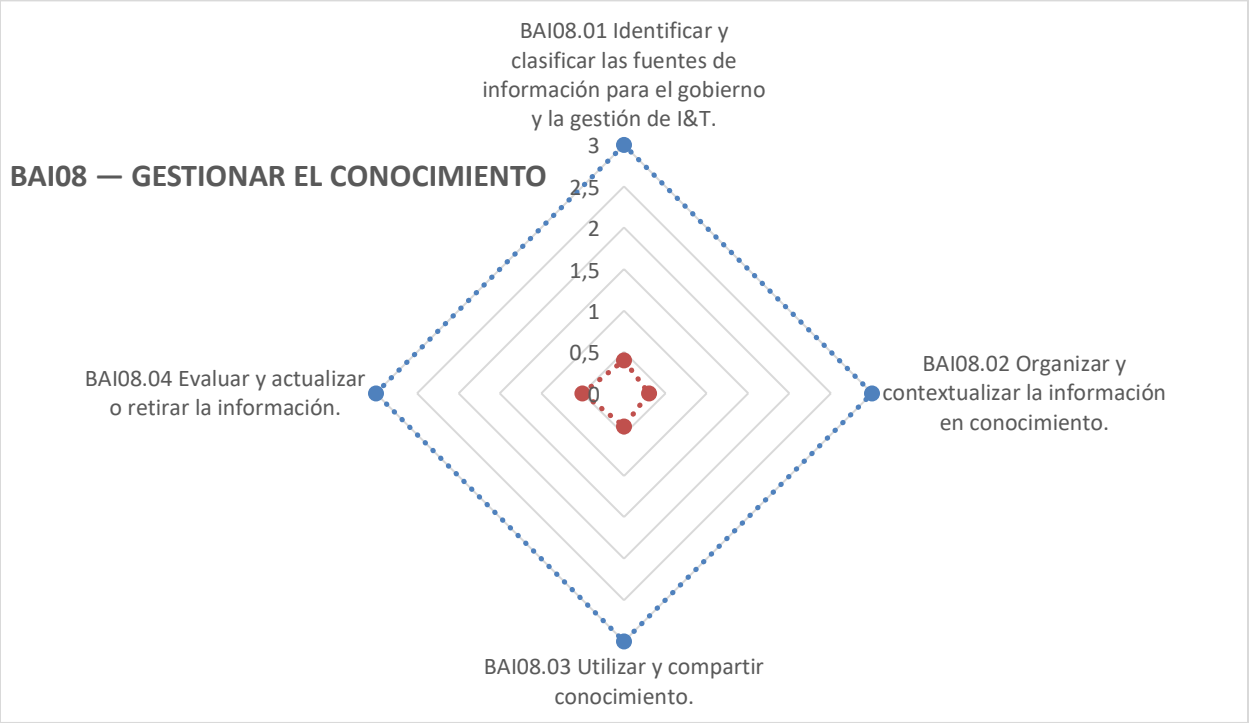


En la segunda practica de gobierno evaluada que hace referencia a la gestión de la seguridad, también evidencia una falta de atención en los aspectos de no tener establecido un sistema de gestión de seguridad de la información (SGSI) (ver Figura 6). La seguridad de la información es un aspecto fundamental en cualquier entorno organizativo, especialmente en un contexto jurídico donde la confidencialidad, integridad y disponibilidad de la información son críticas.

La ausencia de un SGSI impide la implementación de medidas estructuradas y consistentes para proteger la información sensible y los datos confidenciales. Esto deja a la institución vulnerable a amenazas internas y externas, como el acceso no autorizado, la manipulación de datos o las violaciones de la privacidad.

Además, la falta de un plan de tratamiento de riesgos de seguridad de la información y privacidad dificulta la identificación y mitigación proactiva de posibles amenazas y vulnerabilidades. Es imperativo que los consultorios jurídicos de las instituciones de educación superior reconozcan la importancia de gestionar la seguridad. Solo mediante el establecimiento de un SGSI sólido, la definición y gestión de un plan de tratamiento de riesgos, y el seguimiento continuo de la seguridad de la información, se puede garantizar la protección efectiva de los datos y la integridad de la institución.

Figura 7.*Comparación de niveles de capacidad de la meta de alineamiento – BAI08.*



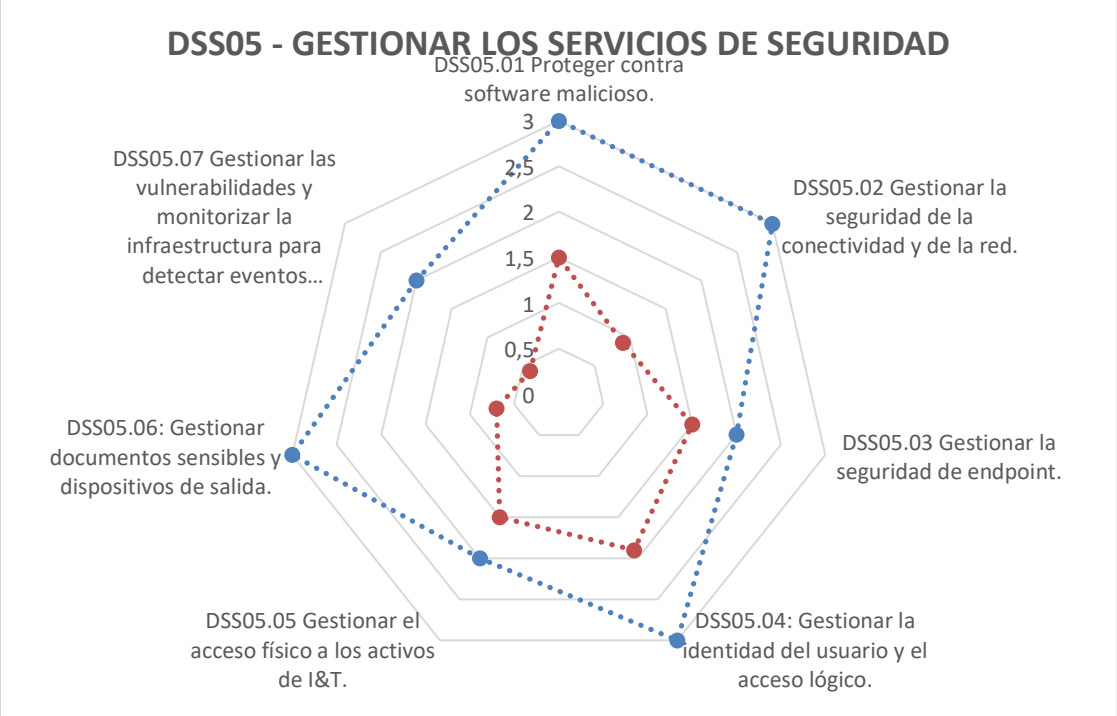
La siguiente practica evaluada es la BAI08 – Gestionar el Conocimiento dentro de los consultorios jurídicos de las IES donde también se ve un bajo nivel de capacidad (ver Figura 7). La gestión del conocimiento es esencial para maximizar el valor de los recursos informativos y promover la eficacia en la toma de decisiones, y los consultorios jurídicos no son la excepción. Sin embargo, en muchos de estos consultorios, se subestima la importancia de esta función crucial.

La falta de identificación y clasificación de fuentes de información impide una comprensión completa de los recursos disponibles, lo que dificulta el acceso y la utilización efectiva de la información relevante.

Además, el no compartir el conocimiento de una manera efectiva dentro del consultorio jurídico resulta en la pérdida de oportunidades para el aprendizaje colaborativo y el intercambio de mejores prácticas entre los miembros del equipo. Esto puede conducir a la duplicación de esfuerzos, la falta de cohesión en la estrategia y la falta de innovación en la prestación de servicios legales.

Por último, la evaluación y actualización de la información se realizan de manera inconsistente y con un seguimiento limitado, lo que puede dar lugar a la obsolescencia de los datos y la falta de alineación con las necesidades cambiantes del consultorio jurídico y sus clientes.

Figura 8.*Comparación de niveles de capacidad de la meta de alineamiento – DSS05.*

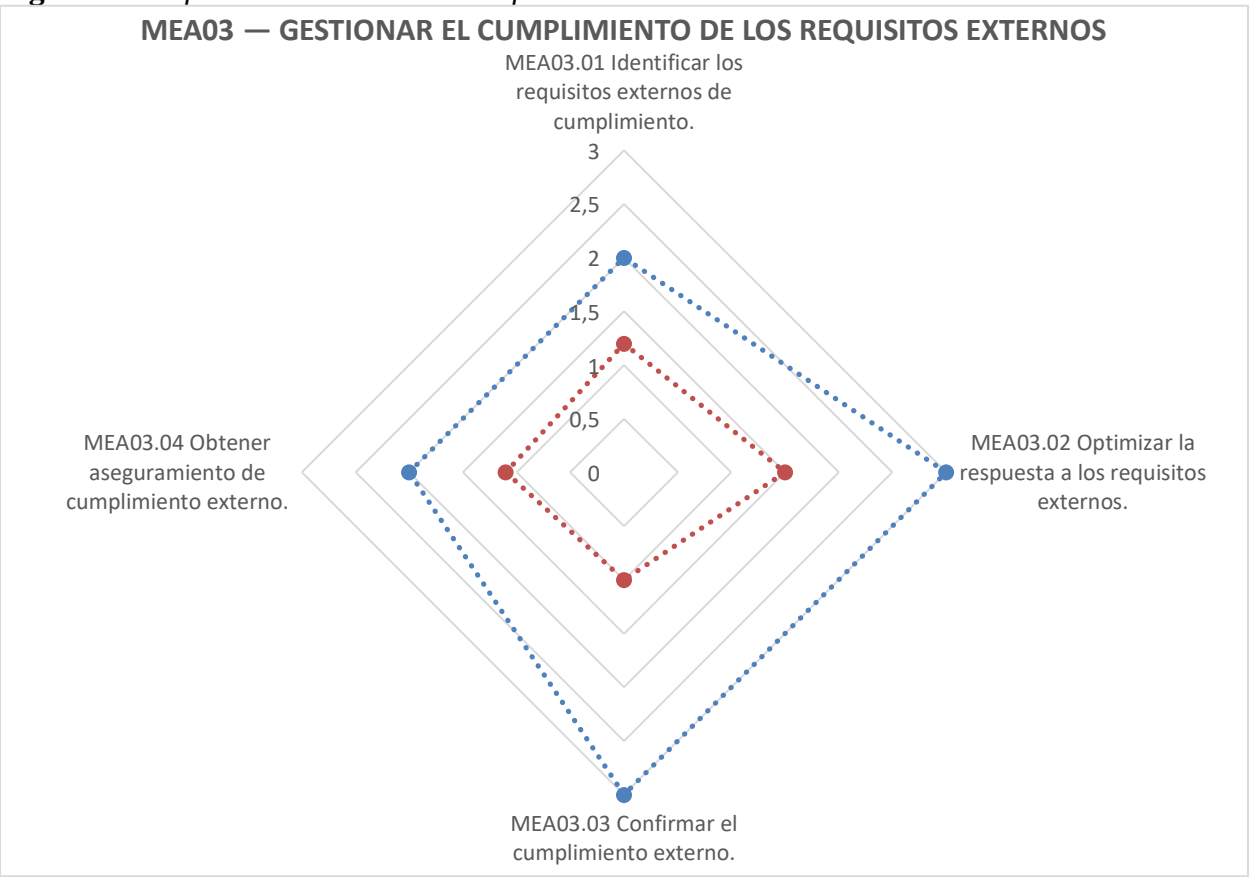


En los consultorios jurídicos de las instituciones de educación superior, se observa un bajo nivel de cumplimiento del objetivo de gestionar los servicios de seguridad aun cuando si realizan algunas actividades requeridas (ver Figura 8). La gestión de los servicios de seguridad es esencial para salvaguardar la integridad, confidencialidad y disponibilidad de la información en un entorno jurídico, donde la seguridad de los datos es de suma importancia.

Si bien se implementan medidas básicas de seguridad, como la protección contra el software malicioso y la gestión de la identidad del usuario, la falta de atención a la gestión de documentos sensibles deja al consultorio vulnerable a posibles filtraciones de información confidencial. Este descuido puede tener graves consecuencias legales y reputacionales para la institución.

Además, la omisión en el seguimiento y monitoreo de estos procesos de seguridad limita la capacidad del consultorio para identificar y responder eficazmente a posibles amenazas y vulnerabilidades. Sin una supervisión constante, es difícil detectar intrusiones o violaciones de seguridad en tiempo real, lo que aumenta el riesgo de incidentes no detectados y el potencial daño a la reputación y la confianza de los usuarios.

Figura 9.*Comparación de niveles de capacidad de la meta de alineamiento – MEA03.*



La última práctica de gobierno evaluada es la de gestionar el cumplimiento de los requisitos externos en los consultorios jurídicos de las IES que se lleva a cabo en cierta medida, pero aún hay margen para mejoras significativas. Si bien se identifican los requisitos externos de cumplimiento y se optimizan las respuestas a estos, así como se confirma el cumplimiento y se obtiene el aseguramiento de cumplimiento, todo el proceso podría mejorar con acciones adicionales.

El cumplimiento de los requisitos externos es fundamental en el ámbito legal, donde las instituciones deben cumplir con una variedad de regulaciones y estándares para garantizar la

transparencia, la legalidad y la ética en sus operaciones. Aunque se realizan ciertas actividades para cumplir con estos requisitos en los consultorios jurídicos, aún se pueden implementar medidas adicionales para fortalecer este proceso.

Por ejemplo, aunque se identifican los requisitos externos de cumplimiento, sería beneficioso realizar una evaluación más exhaustiva y regular para estar al tanto de los cambios en las leyes y regulaciones pertinentes. Además, la optimización de las respuestas a estos requisitos podría incluir la implementación de procedimientos más eficientes y efectivos para garantizar el cumplimiento en todas las áreas relevantes del consultorio jurídico.

En resumen, si bien se realizan esfuerzos para gestionar el cumplimiento de los requisitos externos en los consultorios jurídicos de las instituciones de educación superior, aún hay oportunidades para mejorar el proceso. Mediante la implementación de acciones adicionales, como evaluaciones más exhaustivas, optimización de respuestas, y mejoras en la confirmación y aseguramiento de cumplimiento, se puede fortalecer la capacidad del consultorio para cumplir de manera efectiva con las regulaciones y estándares aplicables.

Los resultados previos se derivaron del uso del instrumento diseñado para diagnosticar el estado actual de la privacidad de la información y la gestión del conocimiento en los consultorios jurídicos de las instituciones de educación superior de Norte de Santander (ver Anexo 2), centrándose específicamente en el componente de procesos que describen una serie de prácticas y actividades organizadas para lograr determinados objetivos y producir una serie de salidas que contribuyan a la consecución de la totalidad de los objetivos relacionados con las TI. Adicional

al componente de los proceso, existen otros componentes del sistema de gobierno (ver Figura 10) que contribuyen al buen funcionamiento del sistema de gobierno que también se evaluaron en el instrumento.

Figura 10.*Componentes del sistema de gobierno.*



4.1.2 Componente de estructuras organizativas

El componente de estructuras organizativas constituye los pilares fundamentales de la toma de decisiones dentro de una organización, definiendo niveles de responsabilidad y rendición de cuentas para las prácticas de los procesos. Al evaluar los resultados obtenidos de la aplicación del instrumento en los consultorios jurídicos de las instituciones de educación superior, se observa que estos consultorios, en su disposición y funcionamiento dentro de las instituciones, heredan algunos roles y características que, aunque no están directamente vinculados a su operación, influyen en su desempeño.

Se destaca que los consultorios jurídicos cumplen al 100% con ciertos roles como el director de TI, la oficina de gestión de proyectos, el asesor legal, el director de recursos humanos y el proceso de auditoría. No obstante, se evidencia una carencia significativa en otros roles cruciales, como el director de riesgos, el director de seguridad de la información, el gestor de seguridad de la información, el director de privacidad, entre otros, los cuales son esenciales para abordar efectivamente el tema de la privacidad de la información.

Es importante resaltar que la ausencia de estos roles clave puede representar un obstáculo significativo para garantizar la protección adecuada de la información confidencial y el cumplimiento de las regulaciones de privacidad. La incorporación de estos cargos en la estructura organizativa de los consultorios jurídicos podría fortalecer su capacidad para gestionar eficazmente los riesgos relacionados con la privacidad de la información y promover una cultura de seguridad sólida dentro de la institución.

4.1.3 Componente de flujos e información

El tercer componente del gobierno, los flujos de información, proporciona una guía sobre los movimientos y elementos de información relacionados con las prácticas de los procesos. Cada práctica incluye entradas y salidas, con indicaciones de su origen y destino. En el instrumento (ver Anexo 2), se define en los consultorios jurídicos si cuentan con las entradas de una estrategia de seguridad, planes de transferencia de conocimiento y requisitos de cumplimiento legal y regulatorio.

En los resultados del componente, se observa que el 100% de los consultorios jurídicos cumplen con identificar los requisitos de cumplimiento legal y regulatorio, así como con algunas características de salida del proceso. Sin embargo, en cuanto a las entradas de estrategias de seguridad y planes de transferencia de conocimiento, solo el 50% cumple con tener identificados los requisitos y algunas características asociadas, aunque estas puedan ser consideradas como pasos iniciales o muy básicos para abordar los requisitos. Por otro lado, el 100% no cumple con las salidas requeridas, como la validación de un sistema de gestión de seguridad de la información, repositorios de conocimiento o la definición de políticas.

Es importante destacar que el cumplimiento de estas salidas es fundamental para garantizar la efectividad de los procesos y la seguridad de la información dentro de los consultorios jurídicos. La implementación de sistemas de gestión de seguridad de la información, la documentación de conocimiento y la definición de políticas son pasos clave para fortalecer la protección de los datos confidenciales y promover buenas prácticas de gestión en estos entornos.

4.1.4 Componente de personas, habilidades y competencia

El componente de personas, habilidades y competencias del marco metodológico de COBIT 2019 identifica los recursos humanos y las habilidades necesarias para lograr los objetivos de gobierno o gestión. En el instrumento de evaluación, se verifica si los consultorios jurídicos cuentan con las personas adecuadas, habilidades y competencias de acuerdo con el listado de características relacionadas con las metas empresariales priorizadas.

Los resultados muestran que el 50% de los consultorios jurídicos encuestados cumplen con habilidades y competencias básicas en la gestión de riesgos de negocios, aseguramiento y proceso de seguridad de la información. Sin embargo, otras características críticas como la gestión de riesgos, el desarrollo de estrategias de seguridad, la gestión de la información y el conocimiento no cuentan con las competencias requeridas para cumplir con los estándares mínimos.

Esto subraya la necesidad de mejorar la capacitación y desarrollo del personal en áreas clave como la gestión de riesgos y la estrategia de seguridad. Además, es crucial invertir en el fortalecimiento de la gestión de la información y el conocimiento, ya que estos aspectos desempeñan un papel fundamental en la protección y optimización de los activos de información dentro de los consultorios jurídicos de las instituciones de educación superior.

4.1.5 Componente de políticas y procedimientos

El componente de políticas y procedimientos se refiere al cumplimiento de normativas y directrices establecidas dentro de las organizaciones. El instrumento de evaluación valida que el 100% de los consultorios jurídicos cumplen con la política de cumplimiento relacionada con el objetivo de gestionar el cumplimiento de los requisitos externos, lo cual puede estar integrado dentro de la estructura misma de los consultorios y su naturaleza legal.

Sin embargo, es preocupante que el 100% de los consultorios no cumplan con políticas cruciales como las de riesgo empresarial, riesgo de fraude, gestión de datos, evaluación de

calidad, privacidad, y uso del conocimiento sobre gobierno y seguridad de la información. Esta falta de cumplimiento demuestra una gran deficiencia en el desarrollo de políticas relacionadas con la privacidad de la información y la gestión del conocimiento en los consultorios jurídicos de las instituciones de educación superior.

Es fundamental destacar que el incumplimiento de estas políticas puede tener graves consecuencias, incluyendo riesgos legales, pérdida de datos confidenciales, daños a la reputación institucional y posibles sanciones regulatorias. Por lo tanto, es imperativo que los consultorios jurídicos tomen medidas urgentes para mejorar el desarrollo, implementación y cumplimiento de políticas que aborden adecuadamente la privacidad de la información y la gestión del conocimiento, garantizando así la integridad y seguridad de los datos en sus operaciones.

4.1.6 Componente de cultura, ética y comportamiento

La cultura, ética y comportamiento tanto de los individuos como de la empresa son a menudo pasados por alto como factores críticos para el éxito en las actividades de gobierno y gestión, según el marco de referencia COBIT 2019. Este componente proporciona una guía detallada sobre los elementos culturales deseados dentro de la organización, destacando la importancia de fomentar una cultura que promueva la integridad, la ética y el compromiso con las mejores prácticas.

Al aplicar el instrumento de evaluación en los consultorios jurídicos, se observa que el 100% de los consultorios encuestados carecen de una cultura relacionada con los objetivos de

gestionar el riesgo y la seguridad, aspectos cruciales para implementar adecuadamente las buenas prácticas de privacidad de la información. En relación con el objetivo de gestionar el conocimiento, solo un consultorio reconoció la implementación de una política de intercambio de conocimiento, mientras que el 100% de los consultorios encuestados sí implementan una cultura de concienciación sobre el cumplimiento de requisitos legales y regulatorios.

Es fundamental destacar la importancia de promover una cultura organizacional que respalde activamente los objetivos de seguridad de la información y gestión del conocimiento. Fomentar una cultura de concienciación y cumplimiento no solo puede mejorar la seguridad de los datos y el cumplimiento normativo, sino que también puede fortalecer la reputación de la institución y su capacidad para enfrentar los desafíos emergentes en el entorno legal y regulatorio. En este sentido, es esencial que los consultorios jurídicos reconozcan la necesidad de cultivar una cultura que valore la seguridad, la ética y el compromiso con la excelencia en todas sus operaciones.

4.1.7 Componente de servicios, infraestructura y aplicaciones

Los servicios, infraestructuras y aplicaciones son elementos clave que pueden utilizarse para respaldar el cumplimiento de los objetivos dentro de una organización. Al aplicar el instrumento en los consultorios jurídicos de las instituciones de educación superior, se confirma que el 100% cumple con sistemas fundamentales como el filtrado de correo electrónico, gestión de acceso e identidad, y filtrado de URL, todos esenciales para su funcionamiento dentro del entorno académico.

Sin embargo, es preocupante observar que los servicios y herramientas relacionados con la gestión de riesgos y el cumplimiento de requisitos externos no están implementados en el 100% de los consultorios encuestados. Esta falta de implementación señala una importante deficiencia en la capacidad de estos consultorios para respaldar y dar seguimiento efectivo a los procesos relacionados con la gestión del riesgo y el cumplimiento normativo.

Es crucial destacar la importancia de contar con servicios y herramientas adecuados para gestionar eficazmente los riesgos y cumplir con los requisitos externos. Estas herramientas no solo ayudan a garantizar la seguridad y el cumplimiento normativo, sino que también son fundamentales para mantener la integridad y confidencialidad de la información dentro de los consultorios jurídicos. Por lo tanto, es fundamental que los consultorios identifiquen y implementen las soluciones adecuadas para abordar estas áreas críticas y asegurar un entorno operativo seguro y conforme con las regulaciones.

4.1.8 Normativa

La normativa no es un componente del marco de referencia COBIT 2019, pero se incluyó en el instrumento para validar el cumplimiento de normas y leyes que apliquen dentro del funcionamiento de los consultorios jurídicos de las instituciones de educación superior. Se valida el cumplimiento de la ley de protección de datos y ley de delitos informáticos, donde el 100% de los consultorios no cumplen con la normativa; por el contrario, la ley 2113 del 2021 que rige el funcionamiento de los consultorios jurídicos se valida que el 100% hacen cumplimiento de la ley.

4.2 Estructura del modelo de privacidad de la información con enfoque en gestión del conocimiento para los consultorios jurídicos de las instituciones de educación superior de Norte de Santander.

Los consultorios jurídicos de las Instituciones de Educación Superior desempeñan un papel fundamental en el cumplimiento de su misión, brindando servicios de asesoría jurídica, representación judicial y extrajudicial a toda la comunidad que cumpla con los requisitos establecidos. En este contexto, es crucial destacar la importancia de salvaguardar la confidencialidad y la integridad de la información proporcionada por los usuarios a los consultorios jurídicos. Cada dato suministrado debe ser manejado con el más alto nivel de cuidado y responsabilidad, garantizando que solo se utilice para los fines legítimos y autorizados.

La información confidencial recibida, que puede incluir datos personales, financieros o de otra índole sensible, debe ser protegida de manera rigurosa contra cualquier forma de acceso no autorizado, divulgación o alteración. Esto implica implementar medidas de seguridad adecuadas, tanto técnicas como organizativas, para proteger esta información contra posibles riesgos como el acceso no autorizado, la divulgación accidental o malintencionada, la pérdida o la destrucción.

Además del deber ético de preservar la confidencialidad de la información de los usuarios, los consultorios jurídicos también están legalmente obligados a cumplir con la normativa y regulaciones pertinentes en materia de privacidad de la información. Esto incluye, entre otras leyes y estándares, la legislación nacional e internacional sobre protección de datos personales y privacidad, así como las políticas institucionales y sectoriales aplicables. En este

sentido, es esencial que los consultorios jurídicos establezcan y mantengan procedimientos claros y efectivos para el manejo seguro de la información, asegurándose de que todo el personal esté debidamente capacitado y consciente de sus responsabilidades en materia de privacidad y seguridad de la información.

Además de la protección de la privacidad, la gestión del conocimiento emerge como un componente crucial para mejorar la eficiencia y la efectividad de los consultorios jurídicos. La gestión del conocimiento implica el proceso de identificar, capturar, organizar, compartir y utilizar el conocimiento y la experiencia de manera efectiva dentro de una organización. En el contexto de los consultorios jurídicos, una sólida gestión del conocimiento puede facilitar la prestación de servicios jurídicos de alta calidad al aprovechar las lecciones aprendidas, las mejores prácticas y los recursos disponibles. Al integrar la gestión del conocimiento con la protección de la privacidad de la información, los consultorios jurídicos pueden fortalecer su capacidad para cumplir con su misión institucional mientras aseguran la confidencialidad y la integridad de los datos de sus usuarios.

4.2.1 Modelo de privacidad de la información con enfoque en gestión del conocimiento para los consultorios jurídicos de las instituciones de educación superior.

Tras comprender la importancia y la complejidad de preservar la privacidad de la información en los consultorios jurídicos de las instituciones de educación superior, así como reconocer el valor estratégico de la gestión del conocimiento en este contexto, surge la necesidad de estructurar un modelo integral que aborde estas áreas de manera efectiva y con las prácticas de gobierno priorizadas y evaluadas en todo el proceso, se define el modelo (ver Figura 11) donde se resaltan 2 prácticas de gobierno, la APO13 – gestionar la seguridad y la BAI08 – gestionar el conocimiento como componentes transversales en todo el modelo y mostrando la importancia que deben tener. Ambas resaltan por su papel crítico y omnipresente en el modelo, evidenciando la trascendencia que deben posesionar.

Simultáneamente, el modelo trae a consideración otras prácticas de gobierno que son vitales para su progreso y cumplimiento efectivo. Estas incluyen APO12 - Gestión de Riesgos, DSS05 - Gestión del Servicio de Seguridad y MEA03 - Gestión del Cumplimiento de Requisitos Externos.

Finalmente, el modelo alude a componentes legales vitales, tales como la Ley 1581 de 2012 - Privacidad de la Información, Ley 1273 del 2009 – Protección de la Información y de los Datos y la Ley 2113 de 2021 - Consultorio Jurídico de las IES. Estos estatutos son normas fundamentales y obligatorias para el funcionamiento de los consultorios jurídicos. A través de las prácticas de gobierno que el modelo ilustra, se facilita su cumplimiento y se garantiza la correcta implementación en el terreno práctico.

Figura 11. *Modelo de privacidad de la información con enfoque en gestión del conocimiento para los consultorios jurídicos de las instituciones de educación superior.*



Para forjar el desarrollo del modelo propuesto, se ha ideado un enfoque estructurado y escalonado, fragmentado en fases meticulosamente delimitadas que garantizan una implementación coherente y exitosa (ver Figura 12).

Las fases establecidas en el modelo son el reconocimiento de la organización, diagnóstico de la privacidad de la información, socialización de los resultados, implementación de prácticas de gobierno y gestión y la mejora continua.

A continuación, se describirá individualmente cada etapa resaltando su relevancia intrínseca dentro del modelo para optimizar las eficiencias del mismo.

Es fundamental recalcar que cada fase desempeña un papel crucial en el proceso de implementación del modelo. Las entradas y salidas de información que se recopilan en cada etapa actúan como insumos esenciales para las etapas subsecuentes, creando un ciclo de realimentación constante y beneficioso.

Figura 12.*Fases del modelo de privacidad de la información con enfoque en gestión del conocimiento para los consultorios jurídicos de las instituciones de educación superior*.



4.2.1.1. Reconocimiento de la organización.

La primera fase, hace referencia al reconocimiento de la organización que se centra en comprender a fondo la estructura, funcionamiento y características particulares de los consultorios jurídicos en las instituciones de educación superior. Esto implica identificar la estructura organizativa, las funciones y servicios ofrecidos, los clientes y beneficiarios de los servicios, los actores claves, los procesos existentes, los recursos disponibles y analizar el contexto institucional y normativo en el que operan.

- **Estructura organizativa:** Describe la organización interna del consultorio jurídico, incluyendo la distribución de responsabilidades y roles dentro del equipo, así como las relaciones jerárquicas y de comunicación.

- **Funciones y servicios ofrecidos:** Detalla los servicios específicos que ofrece el consultorio jurídico, como la asesoría legal, representación judicial, mediación, entre otros. También es importante considerar a quién van dirigidos estos servicios y cómo se gestionan las solicitudes de asistencia legal.

- **Clientes y beneficiarios:** Identifica quiénes son los principales clientes o beneficiarios del consultorio jurídico, como estudiantes, personal administrativo, miembros de la comunidad local, entre otros. Analiza sus necesidades y expectativas en cuanto a los servicios legales ofrecidos.

- **Recursos disponibles:** Evalúa los recursos humanos, financieros, tecnológicos y físicos disponibles para el funcionamiento del consultorio jurídico. Esto incluye el personal disponible, el presupuesto asignado, la infraestructura física y las herramientas tecnológicas utilizadas.

- **Contexto institucional y normativo:** Examina el contexto más amplio en el que opera el consultorio jurídico, considerando las políticas y regulaciones institucionales, así como la legislación nacional relacionada con la prestación de servicios legales en el ámbito educativo.

- **Información sensible:** Identifica la información y datos sensibles de los usuarios como información personal, financiera o legalmente protegida comprendiendo los riesgos y requisitos de privacidad asociados al manejo de la información.

4.2.1.2. Diagnóstico de privacidad de la información.

Esta fase implica una evaluación de la situación actual en cuanto a la privacidad de la información y la gestión del conocimiento en los consultorios jurídicos. Se realizan análisis detallados de los sistemas de gestión de la información, las políticas de privacidad existentes, los niveles de conciencia y capacitación del personal, entre otros aspectos relevantes.

Para realizar el diagnóstico se utilizará un cuestionario basado en la escala Likert. Este cuestionario ha sido diseñado teniendo en cuenta los aspectos más relevantes de la privacidad de la información y la gestión del conocimiento, guiados por el marco de referencia COBIT 2019 y las leyes 1581 del 2012, 1273 del 2009 y la 2113 del 2021.

El uso de la escala Likert permite obtener respuestas no binarias, proporcionando un mayor detalle de las percepciones existentes. En lugar de limitarse a identificar si se cumplen o no ciertos aspectos, la escala Likert permitirá evaluar el grado en que estos aspectos están instaurados en la organización. Esto ofrece una comprensión más profunda de las potenciales áreas de mejora y podría ayudar a identificar oportunidades específicas para fortalecer la privacidad de la información y las prácticas de gestión del conocimiento.

- **Privacidad de la información:** Analiza las prácticas y políticas actuales relacionadas con la protección de la información en el consultorio jurídico. Esto incluye la recopilación, almacenamiento, uso, transmisión y disposición de la información, así como las medidas de seguridad implementadas para protegerla.

- **Gestión del conocimiento:** Evalúa cómo se maneja el conocimiento dentro del consultorio jurídico, incluyendo la captura, almacenamiento, distribución y utilización efectiva de la información y la experiencia acumulada. Examina si existen sistemas o procesos formales para gestionar el conocimiento y cómo se fomenta el aprendizaje y la colaboración entre el personal.

- **Identificación de riesgos y desafíos:** Identifica los principales riesgos y desafíos relacionados con la privacidad de la información y la gestión del conocimiento en el consultorio jurídico. Esto puede incluir vulnerabilidades en la seguridad de la información, brechas en el cumplimiento de normativas, falta de conciencia o capacitación del personal, entre otros.

- **Oportunidades de mejora:** Busca oportunidades de mejora en las prácticas actuales de privacidad de la información y gestión del conocimiento. Esto puede incluir la implementación de nuevas políticas o procedimientos, la adopción de tecnologías innovadoras, la capacitación del personal o la mejora de la infraestructura tecnológica.

Al profundizar en estos aspectos, podrás identificar áreas clave de fortaleza y oportunidades de mejora en cuanto a la privacidad de la información y la gestión del conocimiento en el consultorio jurídico, lo cual es fundamental para el diseño y la implementación efectiva del modelo propuesto.

4.2.1.3. Socialización de resultados.

En esta tercera fase, el objetivo principal es compartir y discutir los hallazgos y conclusiones derivados del diagnóstico de la privacidad de la información con todos los actores

involucrados en los consultorios jurídicos. Los aspectos para considerar en esta fase son una comunicación efectiva, sesiones de socialización, retroalimentación, generación de compromisos y un proceso de sensibilización y capacitación.

- **Comunicación efectiva:** Diseña un plan de comunicación que incluya los resultados del diagnóstico y los objetivos del proyecto. Define los medios de comunicación adecuados y los mensajes clave para llegar a todos los stakeholders relevantes en el consultorio jurídico.

- **Jornadas de socialización:** Organiza sesiones de trabajo o reuniones donde se presenten y discutan los resultados del diagnóstico con el personal del consultorio jurídico, incluyendo directivos, abogados, personal administrativo y estudiantes. Fomenta la participación activa y el intercambio de ideas.

- **Feedback y retroalimentación:** Fomenta un ambiente abierto y receptivo donde se pueda recibir feedback y comentarios constructivos sobre los resultados del diagnóstico. Escucha las preocupaciones, sugerencias y puntos de vista de todos los participantes y ten en cuenta sus opiniones en el diseño del modelo propuesto.

- **Generación de compromisos:** Promueve la generación de compromisos por parte de todos los actores involucrados para apoyar la implementación del modelo de privacidad de la información y gestión del conocimiento. Establece metas claras y realistas y define acciones concretas para alcanzarlas.

- **Sensibilización y capacitación:** Proporciona información y capacitación sobre los temas de privacidad de la información y gestión del conocimiento para aumentar la conciencia y el entendimiento de todos los participantes. Esto puede incluir sesiones de formación, materiales informativos y recursos educativos.

Al socializar los resultados del diagnóstico de manera efectiva, podrás obtener el apoyo y la colaboración necesarios de todos los actores involucrados en el consultorio jurídico, lo cual es fundamental para la implementación exitosa del modelo propuesto.

4.2.1.4 Implementación de prácticas de gobierno y gestión.

Esta etapa posee una importancia crucial debido a que, mediante su aplicación efectiva, se logra avanzar sustancialmente en el logro y optimización de la privacidad de la información en los consultorios jurídicos de las IES. Todo esto se basa en las prácticas de gobierno y gestión conceptualizadas específicamente en el contexto de los consultorios jurídicos, enfatizando aquellos componentes que requieren priorización. En consonancia con el procedimiento llevado a cabo y los objetivos de gobierno y gestión seleccionados como prioritarios, se listan las actividades que a continuación se detallan:

- **Política de privacidad:** Establecer y documentar una política de privacidad detallada, comunicar regularmente la política de privacidad a todos los miembros de la organización y actualizar la política de privacidad para abordar cualquier cambio en las leyes y regulaciones.
- **Responsable de privacidad:** Designar a un individuo o equipo para supervisar la privacidad de la información.

- **Evaluaciones y auditorías:** Implementar un programa para realizar evaluaciones y auditorías de riesgos de privacidad regularmente.
- **Gestión de incumplimientos:** Establecer un proceso para reportar y gestionar incumplimientos de privacidad.
- **Procesos de consentimiento:** Implementar procesos para obtener consentimiento antes de recolectar, usar o divulgar información personal.
- **Controles de acceso:** Implementar controles de acceso para limitar quién puede acceder a la información personal.
- **Programas de formación en privacidad:** Proporcionar formación regular en privacidad de la información a todos los miembros de la organización.
- **Destrucción segura:** Implementar procedimientos para la destrucción segura de la información personal que ya no se necesita.
- **Acceso a la información:** Gestionar adecuadamente el acceso de las personas a su propia información personal.
- **Medidas de seguridad:** Implementar medidas de seguridad para proteger la información personal.
- **Peticiones, quejas y reclamos:** Establecer procedimientos claros para responder a las consultas y quejas sobre privacidad.
- **Seguimiento y control de la privacidad:** Realizar seguimientos y revisiones regulares de las prácticas y políticas de privacidad.
- **Estrategia de gestión del conocimiento:** Diseñar y comunicar una estrategia clara de gestión del conocimiento.

- **Procedimientos de recopilación y almacenamiento:** Establecer procedimientos para recoger, almacenar y acceder al conocimiento.
- **Acceso al conocimiento:** Garantizar que los miembros de la organización pueden acceder fácilmente al conocimiento cuando lo necesitan.
- **Creación de conocimiento y colaboración:** Fomentar la creación de conocimiento y la colaboración entre los miembros de la organización.
- **Seguimiento y evaluación:** Realizar un seguimiento y evaluación regular de las políticas y prácticas de gestión del conocimiento.

Todas las características listadas están alineadas a las prácticas de gobierno y gestión de la siguiente forma:

Política de privacidad / Responsable de privacidad / Evaluaciones y auditorías / Gestión de violaciones / Procesos de consentimiento / Controles de acceso / Formación / Destrucción segura / Acceso a la información / Medidas de seguridad / Respuesta a consultas y quejas / Monitorización y revisión: Estos aspectos están cubiertos por varios objetivos de COBIT 2019, incluyendo APO013 (Gestionar la seguridad), APO012 (Gestionar el riesgo), DSS05 (Gestionar los servicios de seguridad), y MEA03 (Gestionar el cumplimiento de los requisitos externos).

Estrategia de gestión del conocimiento / Procedimientos de recopilación y almacenamiento / Acceso al conocimiento / Creación de conocimiento y colaboración / Seguimiento y evaluación: Estos aspectos se alinean con el objetivo de COBIT BAI08 (Gestionar el conocimiento).

4.2.1.5 Mejora continua.

El proceso de mejora continua es fundamental para garantizar la eficacia y la relevancia continua del modelo de privacidad de la información con enfoque en gestión del conocimiento en los consultorios jurídicos de las instituciones de educación superior. Esta fase se centra en la evaluación periódica de los resultados obtenidos, la identificación de oportunidades de mejora y la implementación de acciones correctivas y preventivas para alcanzar y mantener niveles óptimos de desempeño. Aquí tienes algunos aspectos clave que podrían integrarse en esta fase:

- **Evaluación de resultados:** Realizar una evaluación exhaustiva de los resultados obtenidos hasta el momento, comparándolos con los objetivos y metas establecidos en el modelo de privacidad de la información. Analizar el grado de cumplimiento de los niveles de capacidad definidos en el marco COBIT 2019 y la efectividad de las acciones implementadas para mejorar la gestión de la privacidad y el conocimiento.

- **Identificación de áreas de mejora:** Identificar áreas específicas donde se han identificado brechas o deficiencias en el cumplimiento del modelo de privacidad de la información y gestión del conocimiento. Esto puede incluir la detección de nuevos riesgos o desafíos, cambios en el entorno operativo o nuevas regulaciones que afecten las prácticas de privacidad y seguridad de la información.

- **Planificación de acciones de mejora:** Desarrollar un plan de acción detallado que incluya medidas correctivas y preventivas para abordar las áreas identificadas de mejora.

Establecer metas claras y alcanzables, así como los recursos necesarios para implementar las acciones de mejora de manera efectiva.

- **Implementación de acciones correctivas y preventivas:** Ejecutar las acciones planificadas para abordar las áreas de mejora identificadas. Esto puede incluir la actualización de políticas y procedimientos, la mejora de la infraestructura tecnológica, la capacitación del personal y la revisión de los controles de seguridad de la información.

- **Monitoreo y revisión continua:** Establecer un proceso de monitoreo y revisión continua para verificar la efectividad de las acciones de mejora implementadas. Utilizar indicadores clave de desempeño (KPIs) para medir el progreso y realizar ajustes según sea necesario para garantizar la alineación con los objetivos del modelo de privacidad de la información. Algunos indicadores pueden ser el tiempo medio de respuesta a incidentes, el número de acciones correctivas y preventivas implementadas, el nivel de capacitación del personal, frecuencia de actualización de políticas y procedimientos, tasa de identificación de brechas y deficiencias durante el cumplimiento del modelo de privacidad y la tasa de cumplimiento de objetivos de privacidad.

Al adoptar un enfoque de mejora continua, los consultorios jurídicos pueden mantenerse ágiles y adaptarse a los cambios en el entorno operativo y las necesidades de los usuarios, garantizando así la eficacia y la relevancia a largo plazo del modelo de privacidad de la información y gestión del conocimiento.

4.3 Validación del modelo propuesto de privacidad de la información en un consultorio jurídico en una institución de educación superior de Norte de Santander.

Astigarraga valora la viabilidad de la opinión de expertos mediante el uso de la evolución estadística, concluyendo que es uno de los enfoques más confiables en el ámbito de los métodos de pronóstico subjetivo, específicamente el método Delphi (Astigarraga, 2003). Este método se destaca por su capacidad para generar consenso entre especialistas a través de múltiples rondas de consulta y retroalimentación. Por esta razón, se ha decidido implementar el método Delphi en el presente proyecto.

4.3.1 Selección de expertos.

Para el presente proyecto se toman 7 expertos, 2 expertos en metodología de la investigación, 3 expertos en buenas prácticas de TI y 2 expertos en los procesos de consultorio jurídico de las instituciones de educación superior. Los expertos requeridos se identifican dentro de la base de datos de los docentes de la Universidad Francisco de Paula Santander sede Ocaña y algunos profesionales con conocimientos de los consultorios jurídicos de las instituciones de educación superior.

El siguiente paso fue la medición del coeficiente de competencia de los expertos seleccionados, que se realiza con el diligenciamiento de una encuesta (ver Anexo 3). En la encuesta se define las relaciones de F1, revisión documental realizada del tema de fuentes nacionales; F2, revisión documental realizada del tema de fuentes internacionales; F3, experiencia en el campo de estudio y F4, la intuición del experto. Los resultados se muestran en la siguiente tabla. (ver Tabla 3).

Figura 13.*Perfil de expertos.*

Grupos	Experto	Nivel Conocimiento	F1	F2	F3	F4
Metodología de la Investigación	1	7	A	M	M	M
	2	8	A	A	M	A
Estándares o buenas prácticas de gobierno	3	9	A	A	A	A
	4	7	M	B	M	M
	5	9	A	A	A	A
Consultorios Jurídicos de las IES	6	8	A	M	A	A
	7	8	A	M	A	A

Fuente: Tomado de Rodríguez, García & García (2017)

El cálculo del coeficiente de competencia experta se efectúa a partir de la opinión mostrada por el experto sobre su nivel de conocimiento acerca del caso de estudio, así como de las fuentes que le permiten argumentar el criterio establecido. Para calcular el coeficiente de competencia se tienen en cuenta la siguiente formula.

$$K = \frac{1}{2}(Kc + Ka)$$

Donde, Kc es el coeficiente de competencia o conocimiento que tiene el experto con referencia al caso de estudio, calculado sobre la valoración del propio experto en una escala de 0 a 10 y múltiplo de 0,1.

Donde Ka es el coeficiente de argumentación o fundamentación de los criterios de los expertos que se obtienen a través de la revisión de la auto evaluación del experto en los grados de influencia de cada fuente según conocimiento y criterio del caso de estudio.

Los resultados de muestran en la siguiente tabla (ver Tabla 4) partiendo del estudio desarrollado por Rodríguez.

Tabla 3.*Fuentes de argumentación del experto vs Grado de influencia de las fuentes.*

Fuentes de Argumentación	Grado de Influencia en cada una de las fuentes		
	A (alto)	M (medio)	B (bajo)
Revisión documental realizada del tema de fuentes nacionales.	0,4	0,2	0,1
Revisión documental realizada del tema de fuentes internacionales.	0,5	0,4	0,2
Experiencia en el campo de estudio.	0,05	0,05	0,05
Su intuición.	0,05	0,05	0,05

Fuente: Tomado de Rodríguez, García & García (2017)

Con referencia a los resultados anteriores, se hace el proceso de cálculo de Kc y Ka. El resultado se observa en la siguiente tabla (ver Tabla 5).

Tabla 4.*Determinación del coeficiente del experto.*

Experto	Grado de Conocimiento	Kc	Patrones				Ka	K = ½ (Kc + Ka)
			F1	F2	F3	F4		
1	7	0,7	0,4	0,4	0,05	0,05	0,90	0,80
2	8	0,8	0,4	0,5	0,05	0,05	1,00	0,90
3	9	0,9	0,4	0,5	0,05	0,05	1,00	0,95
4	8	0,8	0,2	0,5	0,05	0,05	0,80	0,80
5	9	0,9	0,4	0,5	0,05	0,05	1,00	0,95
6	8	0,8	0,4	0,4	0,05	0,05	0,90	0,85
7	8	0,8	0,4	0,4	0,05	0,05	0,90	0,85

Fuente: Elaboración propia

Con la información de la tabla 5 se determinó el coeficiente del experto, lo cual se requiere para obtener el coeficiente de competencia. El coeficiente de competencia del experto se establece con ayuda de la siguiente tabla (ver Tabla 6) que define la comparación del coeficiente contra unos rangos, para poder determinar el coeficiente de competencia.

Tabla 5.*Rangos para definición de coeficiente de competencia.*

Variable	Rango	Coeficiente de Competencia
K	Se encuentra entre 0,8 y 1	Alto
K	Se encuentra entre 0,5 y 0,8	Medio
K	Se encuentra menor de 0,5	Bajo

Fuente: Elaboración propia

7 expertos obtuvieron el coeficiente de competencia ALTO y 3 expertos un coeficiente MEDIO. Para el seguimiento de la validación se toman los expertos con coeficiente de competencia alto. A continuación, se pasa a medir el grado de factibilidad de las fases del modelo propuesto, con base los perfiles de los expertos que se detallan en la siguiente tabla (ver Tabla 7).

Tabla 6.*Perfiles de los expertos.*

Experto	Institución	Calificación Profesional	Años Experiencia
Claudia Gómez	Universidad Francisco de Paula	Magister	13
Yesica Pérez	Universidad Francisco de Paula Ocaña	Magister	8
Torcoroma Velásquez	Universidad Francisco de Paula Ocaña	Post Doctora	28
Carlos Rene Angarita	Universidad Francisco de Paula	Magister	10
Hugo Fernando Castro	Universidad Pedagógica y Tecnológica de Colombia	Magister	25
Yusmar Peña	Universidad Simón Bolívar	Magister	21
Eliana Mora	Universidad Simón Bolívar	Magister	20

Fuente: Elaboración propia

4.3.2 Evaluación del modelo.

Una vez seleccionados los expertos que cumplen con la valoración ALTA, se procede a la siguiente fase, que es la validación del modelo (ver Anexo 6). El objetivo principal fue evaluar la percepción de los expertos encuestados sobre diferentes aspectos del modelo propuesto, desde su capacidad para cumplir con objetivos hasta su adaptabilidad en contextos específicos como consultorios jurídicos de las instituciones de educación superior.

Primero, se procede con el cálculo de las frecuencias absolutas (ver Tabla 8) y relativas (ver Tabla 9) para cada pregunta. Esto nos permite cuantificar y comparar la distribución de respuestas en categorías que van desde "Muy Relevante" hasta "Nada Relevante". Este análisis brindó una visión clara de la percepción predominante entre los encuestados en relación con cada aspecto evaluado del modelo.

Tabla 7.*Resultados de frecuencia absoluta*.

Preguntas	MR	BR	R	PR	NR	Total
El modelo permite cumplir con el objetivo propuesto.	7	0	0	0	0	7
El modelo se sustenta en estándares reconocidos y normativas vigentes.	7	0	0	0	0	7
Existe pertinencia en los elementos incorporados en el modelo.	7	0	0	0	0	7
El modelo podría ser adaptado a un consultorio jurídico de una IES.	6	1	0	0	0	7

Fuente: Adaptación de Rodríguez, García & García (2017)

Tabla 8.*Resultados de frecuencia relativa.*

Preguntas	R	R		R	R
El modelo permite cumplir con el objetivo propuesto.	.00	.00	.00	.00	
El modelo se sustenta en estándares reconocidos y normativas vigentes.	.00	.00	.00	.00	
Existe pertinencia en los elementos incorporados en el modelo.	.00	.00	.00	.00	
El modelo podría ser adaptado a un consultorio jurídico de una IES.	.75	.25	.00	.00	

Fuente: Adaptación de Rodríguez, García & García (2017)

Posteriormente, se procede a calcular la frecuencia relativa acumulada (ver Tabla 10). Esta medida se utiliza como una métrica fundamental para evaluar si cada pregunta cumple con la valoración esperada. La frecuencia relativa acumulada permite observar la proporción acumulativa de respuestas que satisfacen ciertos criterios, lo que facilita la identificación de tendencias y patrones en los datos recolectados.

Utilizando esta métrica, se puede determinar de manera precisa y cuantitativa si los resultados obtenidos para cada pregunta están alineados con los objetivos esperados. De esta forma, se asegura una validación rigurosa del modelo propuesto. En consecuencia, la frecuencia relativa acumulada no solo sirve para validar individualmente cada pregunta, sino que también contribuye a la validación global del modelo, garantizando su confiabilidad y efectividad.

Tabla 9.*Resultados de frecuencia relativa acumulada.*

Preguntas	MR	BR	R	PR	NR	Total
El modelo permite cumplir con el objetivo propuesto.	1.00	1.00	1.00	1.00	1.00	1.00
El modelo se sustenta en estándares reconocidos y normativas vigentes.	1.00	1.00	1.00	1.00	1.00	1.00
Existe pertinencia en los elementos incorporados en el modelo.	1.00	1.00	1.00	1.00	1.00	1.00
El modelo podría ser adaptado a un consultorio jurídico de una IES.	0.75	1.00	1.00	1.00	1.00	1.00

Fuente: Adaptación de Rodríguez, García & García (2017)

4.3.3 Validación del modelo.

Al hacer un análisis de los datos registrados en la tabla anterior de la frecuencia relativa acumulada, se puede confirmar la validación del modelo propuesto por los expertos consultados durante el proceso de validación. Al verificar los resultados, se observa que la mayoría de las respuestas para cada pregunta han sido calificadas como "Muy Relevante". Este resultado es un indicativo claro de que los expertos consideran que las preguntas y, por extensión, el modelo en su totalidad, cumplen con los criterios de relevancia y precisión esperados.

La alta concentración de respuestas en la categoría de "Muy Relevante" refuerza la solidez y validez del modelo propuesto. Este nivel de consenso entre los expertos validadores proporciona una fuerte evidencia de la efectividad y aplicabilidad del modelo en el contexto para el cual fue diseñado.

Por lo tanto, se puede concluir con confianza que el modelo ha sido validado satisfactoriamente. Este respaldo por parte de los expertos asegura que el modelo es adecuado para su implementación y que cumple con los estándares de calidad y relevancia requeridos.

Además, este modelo fue socializado durante el X Congreso Internacional Dossier 2024, recibiendo una acogida muy favorable por parte de los participantes del evento (ver Anexo 7). agregando un aval adicional que respalda la viabilidad y pertinencia del modelo propuesto.

En el proceso de evaluación del modelo por parte de los expertos, se identifican algunas recomendaciones y comentarios del modelo que se consideran pertinentes. Algunas de las recomendaciones son las siguientes:

- Ser específico en las entradas y salidas para cada una de las fases.
- Indicar cuales KPIs pueden ser aplicables para la fase de monitoreo y mejora continua.
- Explicar mejor como hacer el diagnóstico.
- Cambiar nombre de ítems para dar claridad de la finalidad.

Estas recomendaciones fueron tomadas en cuenta para hacer ajustes al modelo.

Conclusiones

Del diagnóstico inicial de los consultorios jurídicos de las instituciones de educación superior de Norte de Santander analizados, se presenta la falta de recopilación de información impidiendo una comprensión completa de los riesgos a los que se enfrenta las instituciones, lo que a su vez dificulta la toma de decisiones informadas. Además, sin un análisis exhaustivo de los riesgos, es imposible priorizarlos y asignar recursos de manera eficiente para mitigarlos.

La ausencia de un SGSI impide la implementación de medidas estructuradas y consistentes para proteger la información sensible y los datos confidenciales. Esto deja a los consultorios jurídicos de las instituciones de educación superior vulnerables a amenazas internas y externas, como el acceso no autorizado, la manipulación de datos o las violaciones de la privacidad.

La falta de identificación y clasificación de fuentes de información impide una comprensión completa de los recursos disponibles, lo que dificulta el acceso y la utilización efectiva de la información relevante. Además, el no compartir el conocimiento de una manera efectiva dentro del consultorio jurídico resulta en la pérdida de oportunidades para el aprendizaje colaborativo y el intercambio de mejores prácticas entre los miembros del equipo. Esto puede conducir a la duplicación de esfuerzos, la falta de cohesión en la estrategia y la falta de innovación en la prestación de servicios legales.

Se diseña el modelo de privacidad de la información con enfoque en gestión de conocimiento para los consultorios jurídicos de las instituciones de educación superior de Norte de Santander resaltando 2 prácticas de gobierno que plantea ISACA, las cuales son la APO13 – gestionar la seguridad y la BAI08 – gestionar el conocimiento, como componentes transversales en todo el modelo y mostrando la importancia que deben tener. Ambas resaltan por su papel crítico y omnipresente en el modelo, evidenciando la trascendencia que deben posesionar.

Simultáneamente, el modelo trae a consideración otras prácticas de gobierno que son vitales para su progreso y cumplimiento efectivo. Estas incluyen APO12 - Gestión de Riesgos, DSS05 - Gestión del Servicio de Seguridad y MEA03 - Gestión del Cumplimiento de Requisitos Externos. Finalmente, el modelo alude a componentes legales vitales, tales como la Ley 1581 de 2012 - Privacidad de la Información, Ley 1273 del 2009 – Protección de la Información y de los Datos y la Ley 2113 de 2021.

El modelo incluye las fases de reconocimiento de la organización, diagnóstico de la privacidad de la información, socialización de los resultados, implementación de prácticas de gobierno y gestión y la mejora continua.

Para la validación del modelo se utilizan tres pares expertos de gobierno de TI, dos expertos en consultorios jurídicos y dos expertos en metodología de la investigación. Se utiliza el método Delphi, el cual mide el coeficiente de los expertos, que en este caso están desde maestría hasta postdoctorado, teniendo amplio conocimiento de referentes nacionales e

internacionales, de prácticas en gobierno y gestión de tecnología de la información. Adicional, dentro de los expertos se cuenta con práctica profesional e investigativa entre 10 y 28 años.

Los resultados obtenidos evidencian una buena valoración del modelo y buenas posibilidades de adaptarlo a los consultorios jurídicos de las instituciones de educación superior del Norte de Santander, de igual manera dan algunas recomendaciones para la mejora del modelo presentado.

Recomendaciones

Socializar el modelo propuesto de privacidad de la información con enfoque en gestión del conocimiento con los diferentes consultorios jurídicos del de las instituciones de educación superior de Norte de Santander para la posibilidad de la implementación de este.

Continuar con la presentación de los resultados de la implementación del modelo en los diferentes consultorios jurídicos de las instituciones de educación superior.

Realizar un proceso de mejora continua a partir de los resultados de la implementación del modelo en los consultorios jurídicos.

Referencias

Ackerman, Sebastian, Com, S. (2013). Metodología de la investigación.

Aprobada la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales. Agencia Española de Protección de Datos. 23 de noviembre de 2018.

Astigarraga, E. (2003). El método Delphi. San Sebastián: Universidad de Deusto. http://ibcm.blog.unq.edu.ar/wp-content/uploads/sites/28/2014/03/Metodo_delphi.pdf

Camargo Barbosa, j. A. (2018). Modelo de gobierno de tratamiento de la información para la empresa colombiana en la globalización en la prospectiva del desarrollo organizacional (doctoral dissertation).

Constitución Política de Colombia [Const]. Art. 15 de julio de 1991 (Colombia)

DW. (2021). Líderes sociales asesinados en Colombia. https://www.dw.com/es/reportan-753-l%C3%ADderes-sociales-asesinados-en-colombiade-2016-a-2020/a-56633685

Espitia Ruíz, J. J. (2016). Evolución de la seguridad de la información en el estado colombiano (Bachelor's thesis, Universidad Piloto de Colombia)

Garavito, C. A. R., & Ángel, V. R. (2018). Asesinatos de líderes sociales en Colombia en 2016-2017: una estimación del universo. De justicia.

https://doi.org/10.15332/25005286.6555 Asuntos Legales. (2021). Quejas por Protección de Datos. https://www.asuntoslegales.com.co/actualidad/en-2020-las-quejas-por-proteccion-dedatos-subieron-27-y-la-sic-emitio-76-sanciones-3120123 Ball, P. D.,

Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales. 17 Oct, 2012 Núm. 48587

Ley 2113 de 2021, Por medio del cual se regula el funcionamiento de los consultorios jurídicos de las instituciones de educación superior. 29 Jul, 2021 Núm. 51750

Ley 1273 de 2009, Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos. 5 enero, 2009 Núm. 47223

Miguélez, M. M. (2005). El método etnográfico de investigación. *Etnografía miguelez*, *16*.

Ministerio de las Tecnologías y las Comunicaciones. (2016). Modelo de Seguridad y Privacidad de la Información. articles-5482_Modelo_de_Seguridad_Privacidad.pdf (mintic.gov.co)

Ministerio de las Tecnologías y las Comunicaciones. (2016). Modelo de Seguridad y Privacidad de la Información. articles-5482_Modelo_de_Seguridad_Privacidad.pdf (mintic.gov.co)

Miranda, F. C., & Rodríguez, F. G. O. (2020). La inestabilidad social en El Catatumbo desde la óptica de la violencia estructural (2010-2018). Revista Colombiana de Ciencias Sociales, 11(2), 562-585.

Montejo, Y. C., & Sousa, H. P. (2021). Gestión documental, Gestión de información y Gestión del conocimiento: nociones e interrelaciones. *Bibliotecas. Anales de investigación*, 222-227.

Nelson Remolina-Angarita, ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?, 16 International Law, Revista Colombiana de Derecho Internacional, 489-524 (2010).

Periñán, I. L. M., & Villegas, G. U. (2011). Gobierno de TI–Estado del arte. *Sistemas & Telemática*, *9*(17), 23-53

Red Valor Compartido. (2020) Trabajos con víctimas, reinsertados y grupos vulnerables https://redvalorcompartido.com/miembros-nodo-caribe-universidad-simon-bolivar/

Rodriguez Garcia & Garcia. (2017). El método Delphi para el procesamiento de los resultados de encuestas a expertos o usuarios en estudios de mercado y en la investigación educacional. Universidad Simón Bolivar.

Romero Rodríguez, G. I. (2021). Función de los consultorios jurídicos en el posconflicto. IUSTA, (54).

Superintendencia de Industria y Comercio. (2019). Sanciones Protección de Datos. Personales 2019. https://www.sic.gov.co/sanciones-proteccion-datos-personales-201

Superintendencia de Industria y Comercio. (2020). Quejas recibidas en el 2020. https://www.sic.gov.co/slider/m%C3%A1s-de-16-mil-quejas-recibi%C3%B3-lasuperindustria-en-2020-por-protecci%C3%B3n-de-datos-personales

Superintendencia de Industria y Comercio. (2020). Sanciones Protección de Datos Personales 2020. https://www.sic.gov.co/sanciones-proteccion-datos-personales-2020

Superintendencia de Industria y Comercio. (2021). Sanciones Protección de Datos Personales 2021. https://www.sic.gov.co/sanciones-proteccion-datos-personales-2021

Triana Acevedo, H. R. Diagnóstico y planeación del modelo de seguridad y privacidad de la información en el Hospital San José de Ortega, Tolima, ESE.

Apéndice

Apéndice A.*Matriz de Operacionalización de variables.*

Propósito	Conceptualización	Dimensión	Subdimensión	Indicador
Diseñar un instrumento que permita diagnosticar el estado actual de privacidad de la información y de la gestión de conocimiento en los consultorios jurídicos de las instituciones de educación superior del Norte de Santander	Privacidad de la información.	Ley 1581 del 2012		
	Protección de la Información y de los Datos.	Ley 1273 del 2009		
	Consultorio Jurídico de las Instituciones de Educación Superior.	Ley 2113 del 2021		
	Gobierno de TI	APO12 Gestionar el Riesgo	APO12.01 Recopilar datos	- Proceso. - Estructuras organizativas. - Flujos y elementos de información. - Personas, habilidades y competencias. - Políticas y procedimientos. - Cultura, ética y comportamiento. - Servicios, infraestructura y aplicaciones.
			APO12.02 Analizar el riesgo	
			APO12.03 Mantener un perfil de riesgo	
			APO12.04 Articular el riesgo	
			APO12.05 Definir un portafolio con acciones de gestión de riesgos	
			APO12.06 Responder al riesgo	
		APO13 Gestionar la Seguridad	APO13.01 Establecer y mantener un sistema de gestión de	

			seguridad de la información (SGSI)	
			APO13.02 Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad	
			APO13.03 Monitorizar y revisar el sistema de gestión de seguridad de la información (SGSI)	
		BAI08 Gestionar el Conocimiento	BAI08.01 Identificar y clasificar las fuentes de información para el gobierno y la gestión de I&T	- Proceso. - Estructuras organizativas. - Flujos y elementos de información. - Personas, habilidades y competencias. - Políticas y procedimientos. - Cultura, ética y comportamiento. - Servicios, infraestructura y aplicaciones.
			BAI08.02 Organizar y contextualizar la información en conocimiento	
			BAI08.03 Utilizar y compartir conocimiento	
			BAI08.04 Evaluar y actualizar o retirar la información	
		DSS05 Gestionar los Servicios de Seguridad	DSS05.01 Proteger contra software malicioso	
			DSS05.02 Gestionar la seguridad de la conectividad y de la red	

			DSS05.03 Gestionar la seguridad de endpoint	
			DSS05.04: Gestionar la identidad del usuario y el acceso lógico	
			DSS05.05 Gestionar el acceso físico a los activos de I&T	
			DSS05.06: Gestionar documentos sensibles y dispositivos de salida	
			DSS05.07 Gestionar las vulnerabilidades y monitorizar la infraestructura para detectar eventos relacionados con la seguridad	
		MEA03 Gestionar el Cumplimiento de los Requisitos Externos	MEA03.01 Identificar los requisitos externos de cumplimiento	
			MEA03.02 Optimizar la respuesta a los requisitos externos	
			MEA03.03 Confirmar el cumplimiento externo	
			MEA03.04 Obtener aseguramiento de	

			cumplimiento externo	

Apendice B.*Instrumento para diagnosticar el estado actual de privacidad de la información y de la gestión de conocimiento en los consultorios jurídicos de las instituciones de educación superior del Norte de Santander.*

NIVEL	DESCRIPCION
NIVEL 0	Falta de cualquier capacidad básica.
	Estrategia incompleta para abordar el propósito de gobierno y gestión.
	La intención de todas las prácticas del proceso puede haberse definido o no.
NIVEL 1	El proceso logra más o menos su propósito a través de la aplicación de un conjunto de actividades incompleto que pueden caracterizarse como iniciales o intuitivas, no muy organizadas.
NIVEL 2	El proceso logra su propósito a través de la aplicación de un conjunto de actividades básicas, pero completas, que pueden caracterizarse como realizadas.
NIVEL 3	El proceso logra su propósito de forma mucho más organizada usando acĺvos para la organización. Los procesos están, por lo general, bien definidos.
NIVEL 4	El proceso logra su propósito, está bien definido, y su rendimiento se mide (de forma cuantitativa).
NIVEL 5	El proceso logra su propósito, está bien definido, su rendimiento se mide para mejorar el desempeño y se persigue la mejora continua.

Teniendo como referencia la tabla de niveles de capacidad y su respectiva descripcion, identificar en cada una de las siguientes actividades el nivel que considere que se tiene en la actualidad dentro del consultorio jurídico.

				NIVEL DE CAPACIDAD						CUMPLE	
	PRACTICA DE GOBIERNO	ACTIVIDAD	NIVEL DESEADO	0	1	2	3	4	5	SI	NO
	APO12.01 Recopilar datos.	Establecer y mantener un método para la recogida, clasificación y análisis de datos relacionados con el riesgo de I&T.	2								
		Registrar datos relevantes y significativos relacionados con los riesgos de I&T en el entorno operativo interno y externo de la empresa.	2								
		Adoptar o definir una taxonomía de riesgo para las definiciones consistentes de escenarios de riesgo y categorías de impacto y probabilidad.	3								
		Registrar datos de eventos de riesgo que han causado o podrían causar impacto en el negocio conforme a las categorías de impacto definidas en la taxonomía de riesgo. Capturar datos relevantes de cuestiones, incidentes, problemas e investigaciones.	3								
		Estudiar y analizar los datos históricos de riesgo de I&T y de pérdidas experimentadas a partir de datos y tendencias externos disponibles, homólogos de la industria a través de logs de eventos de la industria, bases de datos, y acuerdos de la industria, para la publicación común de eventos.	4								
		Para clases de eventos similares, organizar los datos recopilados y resaltar los factores causantes. Determinar los factores causantes comunes en múltiples eventos.	4								
		Determinar las condiciones específicas que existieron o estuvieron ausentes cuando tuvieron lugar los eventos de riesgo y la forma en que las condiciones afectaron a la frecuencia del evento y la magnitud de la pérdida.	4								
		Realizar un análisis periódico de eventos y factores de riesgo para identificar riesgos nuevos o emergentes y para mejorar el entendimiento de los factores de riesgo internos y externos asociados.	4								
APO12—Gestionar el Riesgo	APO12.02 Analizar el riesgo.	Definir el alcance adecuado de los esfuerzos en análisis de riesgos, considerando todos los factores de riesgo y/o la criticidad de los activos para el negocio.	3								
		Crear y actualizar regularmente los escenarios de riesgo de I&T; las exposiciones a pérdidas relacionadas con I&T; y los escenarios relacionados con el riesgo reputacional, incluidos escenarios compuestos de tipos de amenazas y eventos en cascada y/o coincidentes. Desarrollar previsiones para actividades de control específicas y capacidades de detección.	3								
		Estimar la frecuencia (o probabilidad) y la magnitud de la pérdida o ganancia asociada con escenarios de riesgos de I&T. Tener en cuenta todos los factores de riesgo aplicables y evaluar controles operativos conocidos.	3								
		Comparar el riesgo actual (exposición a pérdidas de I&T) con el apetito al riesgo y la tolerancia de riesgo aceptable. Identificar el riesgo inaceptable o elevado.	3								
		Proponer respuestas al riesgo para riesgos que excedan el apetito al riesgo y los niveles de tolerancia.	3								
		Especificar los requisitos de alto nivel para los proyectos o programas que implementarán las respuestas a los riesgos seleccionadas. Identificar los requisitos y expectativas para los controles clave adecuados a fin de proporcionar respuestas de mitigación de riesgos.	3								
		Validar el análisis de riesgo y los resultados del análisis de impacto del negocio (BIA) antes de usarlos en la toma de decisiones. Confirmar que el análisis se corresponde con los requisitos empresariales y comprobar que los sesgos de las estimaciones se calibraron y analizaron de forma adecuada.	4								
		Analizar el coste/beneficio de las posibles opciones de respuesta al riesgo, como evitar, reducir/mitigar, transferir/compartir y aceptar y explotar/ aprovechar. Confirmar la respuesta óptima al riesgo.	5								
	APO12.03 Mantener un perfil de riesgo.	Hacer un inventario de los procesos de negocio y documentar su dependencia con los procesos de gestión de servicios de I&T y los recursos de infraestructura de TI. Identificar el personal de apoyo, aplicaciones, infraestructura, instalaciones, registros manuales críticos, contratistas, proveedores, y terceros.	2								
		sostener el funcionamiento de los procesos de negocio. Analizar las dependencias e identificar los eslabones débiles.	2								
		Agregar los escenarios de riesgos actuales por categoría, línea de negocio y área funcional.	2								
		Capturar regularmente toda la información del perfil de riesgo y consolidarla en un perfil de riesgo	3								
		Capturar información sobre el estado del plan de acción de riesgos para su inclusión en el perfil de riesgo de I&T de la empresa.	3								
		Con base en todos los datos del perfil de riesgo, definir un conjunto de indicadores de riesgo que permitan una identificación y monitorización rápida del riesgo actual y las tendencias de riesgo.	4								
		Capturar información sobre eventos de riesgo de I&T que se han materializado para su inclusión en el perfil de riesgo de TI de la empresa.	4								

	APO12.04 Articular el riesgo.	Informar sobre los resultados del análisis de riesgo a todas las partes interesadas afectadas en términos y formatos útiles para soportar las decisiones empresariales. Siempre que sea posible, incluir las probabilidades y rangos de pérdidas o ganancias, junto con los niveles de confianza, para permitir que la gerencia haga balance del retorno del riesgo.	3								
		Proporcionar a los responsables de la toma de decisiones la comprensión de los escenarios más probables y peores, exposiciones a pérdidas de I&T y consideraciones significativas de reputación, legales y regulatorias, o cualquier otra categoría de impacto conforme a la taxonomía de riesgos.	3								
		Informar sobre el perfil de riesgo actual a todas las partes interesadas. Incluir información sobre la eficacia del proceso de gestión de riesgos, eficacia del control, brechas, inconsistencias, redundancias, estado de remediación y sus impactos en el perfil de riesgo.	3								
		oportunidades relacionadas con I&T que permitirían la aceptación de un riesgo mayor y un mayor crecimiento y retorno.	3								
		aseguramiento de la calidad. Incluirlos en el perfil de riesgo. Revisar las brechas identificadas y las exposiciones de pérdidas relacionadas con I&T para determinar la necesidad de un análisis de riesgos adicional.	4								
	APO12.05 Definir un portafolio con acciones de gestión de riesgos.	Mantener un inventario de las actividades de control que se han implantado para mitigar el riesgo y que permiten que se tomen riesgos alineados con el apetito y la tolerancia al riesgo. Clasificar las actividades de control y asignarlas a escenarios de riesgos de I&T específicos y escenarios de riesgos de I&T agregados	2								
		Determinar si cada entidad organizativa monitoriza el riesgo y acepta la responsabilidad de actuar dentro de los niveles de tolerancia individuales y del portafolio.	3								
		Definir un conjunto de propuestas de proyectos equilibrada diseñada para reducir el riesgo y/o proyectos que permitan oportunidades empresariales estratégicas, con consideración de los costes, beneficios, efecto en el perfil de riesgo actual y en las regulaciones.	3								
	APO12.06 Responder al riesgo.	Preparar, mantener y probar planes que documenten los pasos específicos que deben darse cuando un evento de riesgo pudiera causar un incidente significativo de desarrollo u operativo con un impacto grave para el negocio. Asegurar que los planes incluyan vías de escalamiento en la empresa.	3								
		Aplicar el plan de respuesta adecuado para minimizar el impacto cuando ocurren incidentes de riesgo.	3								
		Clasificar los incidentes y comparar las exposiciones a pérdidas relacionadas con I&T con los umbrales de tolerancia al riesgo. Comunicar los impactos de negocio a los responsables de la toma de decisiones como parte del reporte y actualización del perfil de riesgo.	4								
		Examinar eventos adversos/pérdidas y oportunidades del pasado no consideradas y determinar las causas raíz.	4								
		Comunicar la causa raíz, requisitos adicionales de respuestas al riesgo y mejoras del proceso a los responsables de la toma de decisiones correspondientes. Asegurar que la causa, requisitos de respuesta y mejora del proceso se incluyan en los procesos de gobierno del riesgo.	5								

APO13—Gestionar la Seguridad	**APO13.01 Establecer y mantener un sistema de gestión de seguridad de la información (SGSI).**	Definir el alcance y los límites del sistema de gestión de seguridad de la información (SGSI) en términos de las características de la empresa, organización, ubicación, activos y tecnología. Incluir detalles y justificación de las exclusiones del alcance.	2								
		Definir un SGSI conforme a la política empresarial y el contexto en el que opera la empresa	2								
		Alinear el SGSI con el enfoque global de la empresa hacia la gestión de la seguridad.	2								
		Obtener la autorización de la dirección para implementar y operar o cambiar el SGSI.	2								
		Preparar y mantener una declaración de aplicabilidad que describa el alcance del SGSI.	2								
		Definir y comunicar los roles y responsabilidades de la gestión de seguridad de la información.	2								
		Comunicar la estrategia de SGSI.	2								
	APO13.02 Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad.	Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con objetivos estratégicos y la arquitectura empresarial. Asegurar que el plan identifique las prácticas de gestión y las soluciones de seguridad apropiadas y óptimas, con los recursos, responsabilidades y prioridades asociados para la gestión de los riesgos de seguridad de la información identificados.	3								
		Mantener, como parte de la arquitectura de la empresa, un inventario de los componentes de la solución establecida para gestionar los riesgos relacionados con la seguridad.	3								
		casos de negocio apropiados que incluyan consideraciones de financiación y asignación de roles y responsabilidades.	3								
		Proporcionar aportes para el diseño y desarrollo de prácticas y soluciones de gestión, seleccionadas en el plan de tratamiento de riesgos de seguridad de la información.	3								
		Implementar programas de formación y concienciación sobre seguridad de la información y privacidad.	3								
		Integrar la planificación, diseño, implementación y monitorización de procedimientos de seguridad de la información y privacidad y otros controles capaces de permitir la prevención, detección rápida de eventos de seguridad y la respuesta a incidentes de seguridad.	3								
		Definir cómo medir la eficacia de las prácticas de gestión seleccionadas. Especificar cómo deben usarse estas medidas para evaluar la eficacia para producir resultados comparables y reproducibles.	4								
	APO13.03 Monitorizar y revisar el sistema de gestión de seguridad de la información (SGSI).	Llevar a cabo revisiones regulares de la eficacia del SGSI. Incluir el cumplimiento de la política y los objetivos del SGSI y revisar las prácticas de seguridad y privacidad.	4								
		Realizar auditorías de SGSI a intervalos planificados.	4								
		Realizar periódicamente una revisión de la gestión del SGSI para asegurar que el alcance sigue siendo adecuado y que se identifican mejoras en el proceso del SGSI.	4								
		Registrar acciones y eventos que podrían tener un impacto en la eficacia o el rendimiento del SGSI.	4								
		Hacer aportes para el mantenimiento de los planes de seguridad para tener en cuenta los hallazgos de las actividades de monitorización y revisión.	5								

ionar el Conocimiento	**BAI08.01 Identificar y clasificar las fuentes de información para el gobierno y la gestión de I&T.**	Identificar usuarios con conocimiento potenciales, incluidos dueños de información que tal vez deban contribuir y aprobar el conocimiento. Obtener requisitos de conocimiento y fuentes de información de los usuarios identificados.	2								
		Considerar los tipos de contenido (procedimientos, procesos, estructuras, conceptos, políticas, reglas, hechos, clasificaciones), artefactos (documentos, registros, video, voz) e información estructurada y no estructurada (expertos, redes sociales, correo electrónico, mensajes de voz, canales RSS (Rich Site Summary)).	2								
		modelo de arquitectura de la información). Correlacionar las fuentes de información con el esquema de clasificación.	3								
		Recopilar, cotejar y validar las fuentes de información con base en los criterios de validación de la información (p. ej., comprensión, relevancia, importancia, integridad, precisión, consistencia, confidencialidad, vigencia y confiabilidad).	4								
	BAI08.02 Organizar y contextualizar la información en conocimiento.	Identificar atributos compartidos y relacionar sus fuentes de información , con la creación de relaciones entre los conjuntos de información (etiquetado de la información).	3								
		Crear vistas de conjuntos de datos relacionados, considerando los requisitos organizativos y de las partes interesadas.	3								
		Idear e implementar un esquema para gestionar el conocimiento no estructurado que no está disponible a través de fuentes formales (p.ej. el conocimiento de expertos).	3								
		Publicar y hacer que el conocimiento sea accesible a las partes interesadas relevantes, conforme a mecanismos de roles y acceso.	3								

BAI08 — Gest	BAI08.03 Utilizar y compartir conocimiento.	Establecer expectativas de gestión y demostrar la actitud adecuada en cuanto a la utilidad del conocimiento y la necesidad de compartir el conocimiento relacionado con el gobierno y la gestión de la I&T de la empresa.	2								
		Identificar usuarios potenciales de conocimiento por medio de la clasificación del conocimiento.	2								
		Transferir el conocimiento a los usuarios del conocimiento, con base en un análisis de brechas de necesidades y técnicas de aprendizaje efectivas. Crear un entorno, herramientas y artefactos que respalden el intercambio y la transferencia de conocimiento. Asegurar que se cuenta con los controles de acceso adecuados, en línea con la clasificación de conocimiento definida.	3								
		Medir el uso de las herramientas y elementos de conocimiento y evaluar el impacto en los procesos de gobierno.	4								
		Mejorar la información y el conocimiento de los procesos de gobierno que muestran brechas de conocimientos.	5								
	BAI08.04 Evaluar y actualizar o retirar la información.	Definir los controles para la retirada de conocimientos y proceder a su retirada como corresponda.	3								
		Evaluar la utilidad, relevancia y valor de los elementos del conocimiento. Actualizar la información desactualizada que podría seguir siendo relevante y valiosa para la organización. Identificar la información relacionada que ya no es relevante para los requisitos de conocimiento de la empresa y retirarla o archivarla conforme a la política.	4								

dad	DSS05.01 Proteger contra software malicioso.	Instalar y activar herramientas de protección contra software malicioso en todas las instalaciones de procesamiento, con archivos de definición de software malicioso que se actualizan según sea necesario (automáticamente o semiautomáticamente).	2								
		Filtrar el tráfico de entrada, como el correo electrónico y las descargas, para protegerlo de información no solicitada (p.ej. spyware, correos electrónicos de phishing).	2								
		Comunicar acerca de concienciación sobre software malicioso y hacer cumplir los procedimientos y responsabilidades de prevención. Impartir formación periódica sobre malware en el uso de correo electrónico e Internet. Formar a los usuarios para que no abran e informen sobre correos electrónicos sospechosos y no instalen software compartido o no aprobado.	3								
		Distribuir todo el software de protección centralmente (versión y parches) usando una configuración centralizada y la gestión de cambios de TI.	3								
		Revisar y evaluar la información sobre nuevas amenazas potenciales (p. ej., revisión de los consejos de seguridad de productos y servicios de proveedores) de forma regular.	4								
	DSS05.02 Gestionar la seguridad de la conectividad y de la red.	Permitir que solo los dispositivos autorizados tengan acceso a la información corporativa y a la red de la empresa. Configurar estos dispositivos para forzar la introducción de contraseña.	2								
		Implementar mecanismos de filtrado de red, como firewalls y software de detección de intrusos. Hacer cumplir las políticas adecuadas para controlar el tráfico entrante y saliente.	2								
		Aplicar protocolos de seguridad aprobados a las conexiones de red.	2								
		Configurar el equipo de red de forma segura.	2								
		Encriptar la información en tránsito de acuerdo a su clasificación.	3								
		Establecer y mantener una política para la seguridad de la conectividad con base en las evaluaciones de riesgo y los requisitos del negocio.	3								
		Establecer mecanismos confiables para apoyar la transmisión y recepción segura de la información.	3								
		Llevar a cabo pruebas de penetración periódicas para determinar la idoneidad de la protección de la red.	4								
		Llevar a cabo pruebas periódicas a la seguridad del sistema para determinar la idoneidad de la protección del sistema.	4								
	DSS05.03 Gestionar la seguridad de endpoint.	Configurar los sistemas operativos de forma segura.	2								
		Implementar mecanismos de bloqueo de dispositivos.	2								
		Gestionar el acceso y control remotos (p.ej. dispositivos móviles, teletrabajo).	2								
		Gestionar la configuración de red de forma segura.	2								
		Implementar el filtrado de tráfico de red en dispositivos de punto final.	2								
		Proteger la integridad del sistema.	2								
		Proporcionar protección física a los dispositivos de punto final.	2								
		Eliminar de forma segura los dispositivos Endpoint.	2								
		Gestionar el acceso malicioso a través del correo electrónico y los navegadores web. Por ejemplo, bloquear determinados sitios web y desactivar los clics a enlaces para los smartphones.	2								
		Encriptar la información almacenada de acuerdo a su clasificación.	3								

DSS05 - Gestionar los Servicios de Seguri	**DSS05.04: Gestionar la identidad del usuario y el acceso lógico.**	Mantener los derechos de acceso de los usuarios de acuerdo con la función del negocio, los requisitos del proceso y las políticas de seguridad. Alinear la gestión de identidades y derechos de acceso con los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad-de-tener y necesidad-de-conocer.	2								
		Administrar oportunamente todos los cambios en los derechos de acceso (creación, modificación y eliminación), basándose únicamente en transacciones aprobadas y documentadas que hayan sido autorizadas por personas designadas por la dirección.	3								
		Segregar, reducir al mínimo necesario y gestionar activamente cuentas de usuario privilegiadas. Asegurar la supervisión de todas las actividades en estas cuentas.	3								
		Identificar de forma unívoca y por roles funcionales todas las actividades de procesamiento de información. Coordinarse con las unidades de negocio para asegurarse de que todos los roles están definidos de manera consistente, incluidos los roles definidos por el propio negocio dentro de las aplicaciones de procesos del negocio.	3								
		Autenticar todo el acceso a activos de información de acuerdo con el rol del individuo o a las reglas del negocio. Coordinarse con las unidades de negocio que gestionan la autenticación dentro de las aplicaciones utilizadas en los procesos de negocio, con el fin de asegurar que los controles de autenticación hayan sido administrados adecuadamente.	3								
		Garantizar que todos los usuarios (internos, externos y temporales) y su actividad en los sistemas de TI (aplicación de negocio, infraestructura de TI, operaciones, desarrollo y mantenimiento de sistemas) se puedan identificar de manera unívoca.	3								
		Mantener un registro de auditoría del acceso a la información dependiendo de su sensibilidad y de los requisitos regulatorios.	3								
		Llevar a cabo revisiones gerenciales periódicas de todas las cuentas y privilegios relacionados.	4								
	DSS05.05 Gestionar el acceso físico a los activos de I&T.	Registrar y monitorizar todos los puntos de entrada a las instalaciones de TI. Registrar a todos los visitantes al sitio, incluidos contratistas y proveedores.	2								
		Asegurar que todo el personal muestra una identificación debidamente autorizada en todo momento.	2								
		Requerir a los visitantes que estén acompañados en todo momento durante su estancia en las instalaciones.	2								
		Restringir y monitorizar el acceso a instalaciones sensibles de TI, mediante el establecimiento de restricciones al perímetro, como vallas, paredes y dispositivos de seguridad en puertas interiores y exteriores.	2								
		Gestionar solicitudes para permitir el acceso debidamente autorizado a las instalaciones de cómputo.	3								
		Garantizar que los perfiles de acceso permanezcan actualizados. Basar el acceso a las instalaciones de TI (sala de servidores, edificios, áreas o zonas) en el cargo y las responsabilidades.	3								
		Realizar formación sobre concienciación de la seguridad de la información física de forma regular.	3								

	DSS05.06: Gestionar documentos sensibles y dispositivos de salida.	Establecer procedimientos para gobernar la recepción, uso, retiro y desecho de documentos sensibles y dispositivos de salida, dentro y fuera de la empresa.	2								
		Asegurar que se han establecido controles criptográficos para proteger información sensible almacenada electrónicamente.	2								
		Asignar privilegios de acceso a documentos sensibles y dispositivos de salida con base en el principio de menor privilegio, manteniendo un equilibrio entre el riesgo y los requisitos del negocio.	3								
		Establecer un inventario de documentos sensibles y dispositivos de salida y realizar reconciliaciones periódicas.	3								
		Establecer salvaguardas físicas adecuadas para documentos sensibles.	3								
	DSS05.07 Gestionar las vulnerabilidades y monitorizar la infraestructura para detectar eventos relacionados con la seguridad.	Usar de forma continua un portafolio de tecnologías, servicios y activos soportados (p. ej., escáneres de vulnerabilidad, fuzzers y sniffers, analizadores de protocolos) para identificar vulnerabilidades de seguridad de la información.	2								
		Definir y comunicar escenarios de riesgo para que se puedan reconocer con facilidad y se pueda entender su probabilidad e impacto.	2								
		Revisar regularmente los logs de eventos para detectar posibles incidentes.	2								
		Garantizar que se creen tickets relativos a incidentes de seguridad de forma oportuna cuando la monitorización identifique posibles incidentes.	2								
		Registrar eventos relacionados con la seguridad y conservar los registros durante el periodo de tiempo apropiado.	3								

MEA03 — Gestionar el Cumplimiento de los Requisitos Externos.	**MEA03.01 Identificar los requisitos externos de cumplimiento.**	Asignar la responsabilidad de identificar y supervisar los cambios en los requisitos legales, regulatorios y otros requisitos contractuales externos, relevantes para el uso de recursos de TI y el procesamiento de la información dentro de las operaciones empresariales y de TI.	2								
		Identificar y evaluar todos los posibles requisitos de cumplimiento y su impacto en las actividades de I&T, en áreas como flujo de datos, privacidad, controles internos, informes financieros, regulaciones específicas de la industria, propiedad intelectual, salud y seguridad en el trabajo.	2								
		terceros relacionados con las operaciones de TI, proveedores de servicio y otros socios comerciales de negocios.	2								
		Definir las consecuencias del incumplimiento.	2								
		Obtener asesoría independiente cuando corresponda, sobre los cambios en la legislación, regulaciones y estándares vigentes.	3								
		Mantener un registro actualizado de todos los requisitos legales, regulatorios y contractuales; de su impacto y las acciones requeridas.	3								
		Mantener un registro global, armonizado e integrado, de los requisitos de cumplimiento externo para la empresa.	3								
	MEA03.02 Optimizar la respuesta a los requisitos externos.	Revisar y ajustar continuamente las políticas, principios, estándares, procedimientos y metodologías para que sean eficaces en garantizar el cumplimiento necesario y abordar el riesgo empresarial. Usar expertos internos y externos, cuando sea necesario.	3								
		Comunicar los requisitos nuevos y modificados a todo el personal relevante.	3								
	MEA03.03 Confirmar el cumplimiento externo.	Evaluar regularmente las políticas, estándares, procedimientos y metodologías organizativas en todas las funciones de la empresa, para garantizar el cumplimiento de todos los requisitos legales y regulatorios relevantes relacionados con el procesamiento de la información.	3								
		Tratar las brechas de cumplimiento en políticas, estándares y procedimientos con las debida oportunidad.	3								
		Evaluar periódicamente los procesos y actividades del negocio y de TI para asegurar el cumplimiento de los requisitos legales, regulatorios y contractuales vigentes.	3								
		Revisar regularmente los patrones recurrentes de fallos de cumplimiento y evaluar las lecciones	4								
		Mejorar las políticas, estándares, procedimientos, metodologías y sus procesos y actividades asociadas con base en la revisión y las lecciones aprendidas.	5								
	MEA03.04 Obtener aseguramiento de cumplimiento externo.	Obtener confirmación periódica del cumplimiento con las políticas internas por parte de los dueños de los procesos de negocio y de TI y los jefes de unidades.	2								
		Realizar periódicamente revisiones internas y externas (independientes, cuando sea posible,) para evaluar los niveles de cumplimiento.	2								
		Si se requiere, obtener declaraciones de los proveedores de servicio externos de I&T sobre sus niveles de cumplimiento con las leyes y regulaciones aplicables.	2								
		Si se requiere, obtener declaraciones de los socios de negocio sobre sus niveles de cumplimiento con leyes y regulaciones aplicables, en la medida en que estén relacionados con las transacciones electrónicas entre empresas.	2								
		Integrar los informes sobre los requisitos legales, regulatorios y contractuales a nivel global de la empresa, involucrando a todas las unidades de negocio.	3								
		Supervisar y comunicar los problemas de incumplimiento y, cuando sea necesario, investigar la causa raíz.	4								

Componente Estructuras Organizativas

CARGO	¿ Existe el cargo en la organizaición ?		CUMPLE		OBSERVACION	DESCRIPCION DEL CARGO
	SI	NO	SI	NO		
Director de Riesgos						Director de más alto rango que rinde cuentas sobre todos los aspectos de la gestión de riesgos de la empresa.
Director de TI						Director de más alto rango que rinde cuentas sobre el alineamiento de las TI y las estrategias del negocio y rinde cuentas por la planificación, gestión de recursos y prestación de servicios y soluciones de I&T.
Director de Tecnologia						Director de más alto rango encargado de los aspectos técnicos de I&T, incluida la gestión y supervisión de decisiones relacionadas con servicios, soluciones e infraestructura de I&T.
Director de Tecnologias Digitales						Director de más alto rango encargado de poner en práctica la transformación digital de la empresa o de las unidades de negocio.
Comité de Riesgos Empresariales						Grupo de ejecutivos que rinden cuentas sobre del nivel de colaboración y consenso requeridos para respaldar las actividades y decisiones de gestión de riesgos empresariales (ERM).
Director de Seguridad de la Informacion						El director de más alto rango que rinde cuentas sobre todos los aspectos de la gestión de seguridad de la empresa.
Dueños del Proceso del Negocio						Persona que rinde cuentas sobre la ejecución de los procesos y/o el logro de los objetivos de los procesos, conducir la mejora de los procesos y aprobar los cambios a los procesos.
Oficina de Gestion de Proyectos						Función responsable de respaldar a los gestores de proyecto y de programa y de recopilar, evaluar y comunicar información sobre la ejecución de los programas y los proyectos que los componen.
Funcion de Gestion de Datos						Función responsable de respaldar los activos de datos de la empresa durante su ciclo de vida y gestionar la estrategia, infraestructura y repositorios de datos.
Jefe de Arquitectura						Persona experta encargada del proceso de arquitectura empresarial.
Jefe de Desarrollo						Persona experta que rinde cuentas sobre los procesos de desarrollo de soluciones de I&T.
Jefe de Operaciones de TI						Persona experta que rinde cuentas sobre los entornos operativos e infraestructura de TI.
Jefe de Administracion de TI						Persona experta que rinde cuentas sobre los registros de I&T y es responsable de apoyar en labores administrativas de I&T.
Gestor de Servicios						Persona que gestiona el desarrollo, la implementación, la evaluación y el mantenimiento continuo de productos y servicios nuevos o ya existentes, para un cliente específico (usuario) o grupo de clientes (usuarios).
Gestor de Seguridad de la Informacion						Persona que gestiona, diseña, supervisa y/o evalúa la seguridad de la información de una empresa.
Gestor de Continuidad del Negocio						Persona que gestiona, diseña, supervisa y/o evalúa la capacidad de continuidad del negocio de una empresa, para garantizar que sus funciones críticas sigan operando después de eventos disruptivos.
Director de Privacidad						Persona responsable de supervisar el riesgo e impacto de las leyes sobre privacidad en el negocio y de dirigir y coordinar la implementación de políticas y actividades que garanticen el cumplimiento de las directivas de privacidad.
Gestor de Portafolio						Persona responsable de dirigir la gestión del portafolio, asegurar una selección adecuada de programas y proyectos y gestionar y supervisar programas y proyectos para obtener un valor óptimo, así como alcanzar los objetivos estratégicos a largo plazo de forma eficaz y eficiente.
Gestor de Programas						Persona responsable de dirigir un programa específico, incluidos la articulación y el seguimiento de las metas y objetivos del programa y la gestión del riesgo y su impacto en el negocio.
Gestor de Proyecto						Persona responsable de dirigir un proyecto específico, incluidos la coordinación y delegación del tiempo, presupuesto, recursos y tareas del equipo del proyecto.
Asesor Legal						Función responsable de la asesoría en asuntos legales y regulatorios.
Director de Recursos Humanos						El director de más alto rango que rinde cuentas sobre la planificación y las políticas relacionadas con los recursos humanos de la empresa.
Director General Ejecutivo						Director de más alto rango- encargado de la gestión global de la empresa.
Director General Financiero						Director de más alto rango que rinde cuentas sobre todos los aspectos de la gestión financiera, incluido el riesgo y los controles financieros, así como de una contabilidad confiable y precisa.
Director de Operaciones						Director de más alto rango que rinde cuenjtas sobre la la operación de la empresa.
Consejo de Gobierno de I&T						Grupo de partes interesadas y expertos que rinden cuentas sobre la dirección de los asuntos y decisiones relacionadas con I&T, incluidas la gestión de inversiones habilitadas por I&T, la obtención de valor y la supervisión del riesgo.
Cumplimiento						Función responsable de asesorar sobre todo el cumplimiento externo.
Auditoria						Función responsable de la realización de auditorías internas.

Componente Flujos e Información

OBJETIVO	PRACTICA DE GESTION	ENTRADAS	¿Existe en la organización?		SALIDAS	¿Existe en la organización?		OBSERVACION
			SI	NO		SI	NO	
APO13: Gestionar la Seguridad	APO13.01 Establecer y mantener un sistema de gestión de seguridad de la información (SGSI).	Estrategia de seguridad de la empresa.			Declaración del alcance de la SGSI.			
					Política de SGSI.			
BAI08: Gestionar el Conocimiento	BAI08.02 Organizar y contextualizar la información en conocimiento.	Planes de transferencia de conocimiento.			Repositorios de conocimiento publicados.			
	BAI08.03 Utilizar y compartir conocimiento.	Componentes de la solución documentados.			Esquemas de concienciación y capacitación.			
MEA03: Gestionar el Cumplimiento de los Requisitos Externos	MEA03.01 Identificar los requisitos externos de cumplimiento.	Requisitos de cumplimiento legal y regulatorio.			Log de acciones de cumplimiento requeridas.			
					Registro de requisitos de cumplimiento.			
	MEA03.02 Optimizar la respuesta a los requisitos externos.				Comunicaciones de cambios en los requisitos de cumplimiento.			
					Políticas, principios, procedimientos y estándares actualizados.			

Componente Personas, Habilidades y Competencias

PERSONAS, HABILIDADES Y COMPETENCIAS		¿ La organización cuenta con la caracteristica ?		CUMPLE		OBSERVACION
		SI	NO	SI	NO	
APO12 - Gestionar el Riesgo, APO13 - Gestionar la Seguridad, BAI08 — Gestionar el Conocimiento, DSS05 - Gestionar los Servicios de Seguridad, MEA03 — Gestionar el Cumplimiento de los Requisitos Externos	Gestion de riesgos de negocio.					
	Aseguramiento de la informacion.					
	Gestion de riesgos.					
	Seguridad de la informacion.					
	Desarrollo de la estrategia de seguridad de la informacion.					
	Gestion de la informacion y el conocimiento.					
	Gestion de seguridad de la informacion.					
	Pruebas de penetracion.					
	Administracion de seguridad.					

Componente Políticas y Procedimientos

POLITICAS Y PROCEDIMIENTOS		¿ La organización cuenta con la politica ?		CUMPLE		OBSERVACION
		SI	NO	SI	NO	
APO12 - Gestionar el Riesgo	Politica de riesgo empresarial.					
	Politica de riesgo de fraude.					
APO13 - Gestionar la Seguridad	Politica de depuracion de datos.					
	Politica de gestion de datos.					
	Politica de evaluacion de la calidad de datos.					
	Politica de privacidad.					
BAI08 — Gestionar el Conocimiento	Politica de uso del conocimiento sobre gobierno.					
DSS05 - Gestionar los Servicios de Seguridad	Politica de seguridad de la informacion.					
MEA03 — Gestionar el Cumplimiento de los Requisitos Externos	Politca de cumplimiento.					

Componente Cultura Ética y Comportamiento

CULTURA, ETICA Y COMPORTAMIENTO		¿ La organización cuenta con la cultura ?		CUMPLE		OBSERVACION
		SI	NO	SI	NO	
APO12 - Gestionar el Riesgo	Con el objeto de respaldar una cultura del riesgo participativa y transparente, la alta dirección deberia establecer el rumbo y mostrar un apoyo visible y genuino a la incorporación de las prácticas de riesgo en toda la empresa. La dirección deberia fomentar una comunicación abierta y la propiedad empresarial sobre los riesgos de negocio relacionados con I&T. Los comportamientos deseables incluyen el alineamiento de politicas conforme al apetito al riesgo definido, comunicación de tendencias de riesgo a la alta dirección y organismos de gobierno de riesgos, recompensa a una gestión de riesgos eficaz y monitorización proactiva de riesgos y progreso con respecto al plan de acción sobre riesgos.					
APO13 - Gestionar la Seguridad	Establecer una cultura de concienciación de seguridad y privacidad que influya de forma positiva en el comportamiento deseado y la implementación real de la politica de seguridad y privacidad en la práctica diaria. Proporcionar las suficientes directrices de seguridad y privacidad, indicar quiénes son los campeones en seguridad y privacidad (incluidos altos ejecutivos, lideres de RR. HH., profesionales de seguridad y/o privacidad) y apoyar y comunicar de forma proactiva los programas, innovaciones y desafios de seguridad y privacidad.					
BAI08 — Gestionar el Conocimiento	Implantar una cultura de intercambio de conocimientos en la empresa. Comunicar proactivamente el valor de los conocimientos para fomentar la creación, uso, reutilización e intercambio de conocimientos. Fomentar el intercambio y transferencia del conocimiento mediante la identificación y aprovechamiento de factores motivadores.					
DSS05 - Gestionar los Servicios de Seguridad	Crear una cultura de concienciación con respecto a la responsabilidad del usuario de mantener prácticas de seguridad y de privacidad.					
MEA03 — Gestionar el Cumplimiento de los Requisitos Externos	Proporcionar una cultura de concienciación sobre el cumplimiento, incluida una tolerancia cero con el incumplimiento de requisitos legales y regulatorios.					

Componente Servicios, Infraestructura y Aplicaciones

SERVICIOS, INFRAESTRUCTURA Y APLICACIONES		¿ La organización cuenta con el servicio, infraestructura o aplicación ?		CUMPLE		OBSERVACION
		SI	NO	SI	NO	
APO12 - Gestionar el Riesgo	Servicios de gestión de crisis.					
	Herramientas de gobierno, riesgo y cumplimiento (GRC).					
	Herramientas de análisis de riesgos.					
	Servicios de inteligencia de riesgos.					
APO13 - Gestionar la Seguridad	Herramientas de gestión de la configuracion.					
	Servicios de concienciación de seguridad y privacidad.					
	Servicios de evaluación de seguridad de terceros.					
BAI08 — Gestionar el Conocimiento	Plataforma de colaboración.					
	Repositorio de conocimientos.					
DSS05 - Gestionar los Servicios de Seguridad	Servicios de directorio.					
	Sistemas de filtrado de correo electrónico.					
	Sistema de gestión de acceso e identidad.					
	Servicios de concienciación sobre seguridad.					
	Herramientas de seguridad de la información y de gestión de eventos (SIEM).					
	Servicios del centro de operaciones de seguridad (SOC).					
	Servicios de evaluación de seguridad de terceros.					
	Sistemas de filtrado de URL.					
MEA03 — Gestionar el Cumplimiento de los Requisitos Externos	Servicios de vigilancia regulatoria.					
	Servicios de evaluación al cumplimiento de terceros.					

Componente Normativa

NORMATIVA		¿ La organización cuenta con la normativa ?		OBSERVACION
		SI	NO	
1581 del 2012. Ley de Proteccion de Datos Personales	Aplicación de los requisitos de proteccion de datos personales con base a la ley 1581 del 2012.			
1273 del 2009. Ley Delitos Informaticos.	Cumplimiento de los requisitos de ley, proteccion de seguridad, la privacidad de la información y los datos personales de sus clientes y usuarios.			
2113 del 2021. Funcionamiento de los Consultorios Juridicos.	Aplicación del marco normativo del funcionamiento del consultorio juridico en las instituciones de educacion superior con base a la ley 2113 del 2021 y el principio de confidencialidad.			

Apendice C.*Evaluación del instrumento de diagnóstico el estado actual de privacidad de la información y de la gestión de conocimiento en los consultorios jurídicos de las instituciones de educación superior del Norte de Santander.*

Validación del Instrumento

Objetivo: Diagnosticar el estado actual de la privacidad de la información en los consultorios jurídicos de las instituciones de educación superior, el instrumento será validado por medio del método Delphi a través de expertos.

Nombre: Claudia Yamile Gómez Llanez
Institución: Universidad Francisco de Paula Santander – Cúcuta

Nombre del último nivel de escolaridad.			
Marque con una **X** el grado de escolaridad con relación a los años de experiencia y cargos que allá tenido.		Tipo de cargo y años de experiencia.	
Grado de Escolaridad		Investigador y/o Docente	Profesional
Profesional	X		5 años
Licenciado			
Especialista			
Magister	X	7 años	
Doctor			
Postdoctoral			

Para validar el instrumento Privacidad de la Información en los Consultorios Jurídicos de las IES, la cual se adjunta para su verificación y posterior valoración.

Por tanto, solicito muy respetuosamente responda la siguiente encuesta teniendo en cuenta las siguientes categorías:

Muy de acuerdo	5
De acuerdo	4
Ni de acuerdo ni en desacuerdo	3
Desacuerdo	2
Totalmente en desacuerdo	1

Marque con una (X) la respuesta correspondiente a la pregunta formulada.

MODELO DE ACTUACIÓN					
	5	4	3	2	1
El instrumento permite cumplir con el objetivo propuesto.	x				
Las preguntas son claras y entendibles.	x				
Las instrucciones son claras para responder las preguntas planteadas.		x			
Las preguntas corresponden con las dimensiones y subdimensiones definidas en la sistematización de variables (ver tabla 1)	x				

Tabla 1. Dimensiones del instrumento

Dimensiones	Subdimensiones	Indicadores
APO12: Gestionar el Riesgo	APO12.01 Recopilar datos.	Procesos. Estructuras Organizativas. Flujos e Información. Personas, Habilidades y Competencias. Políticas y Procedimientos. Cultura, Ética y Comportamiento. Servicios, Infraestructura y Aplicación.
	APO12.02 Analizar el riesgo.	
	APO12.03 Mantener un perfil de riesgo.	
	APO12.04 Articular el riesgo.	
	APO12.05 Definir un portafolio con acciones de gestión de riesgos.	
	APO12.06 Responder al riesgo.	
APO13: Gestionar la Seguridad	APO13.01 Establecer y mantener un sistema de gestión de seguridad de la información (SGSI).	Procesos. Estructuras Organizativas. Flujos e Información. Personas, Habilidades y Competencias. Políticas y Procedimientos. Cultura, Ética y Comportamiento. Servicios, Infraestructura y Aplicación.
	APO13.02 Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad.	
	APO13.03 Monitorizar y revisar el sistema de gestión de seguridad de la información (SGSI).	
BAI08: Gestionar el Conocimiento	BAI08.01 Identificar y clasificar las fuentes de información para el gobierno y la gestión de I&T.	Procesos. Estructuras Organizativas. Flujos e Información. Personas, Habilidades y Competencias. Políticas y Procedimientos. Cultura, Ética y Comportamiento. Servicios, Infraestructura y Aplicación.
	BAI08.02 Organizar y contextualizar la información en conocimiento.	
	BAI08.03 Utilizar y compartir conocimiento.	
	BAI08.04 Evaluar y actualizar o retirar la información.	
DSS05 - Gestionar los Servicios de Seguridad	DSS05.01 Proteger contra software malicioso.	Procesos. Estructuras Organizativas. Flujos e Información. Personas, Habilidades y Competencias. Políticas y Procedimientos. Cultura, Ética y Comportamiento. Servicios, Infraestructura y Aplicación.
	DSS05.02 Gestionar la seguridad de la conectividad y de la red.	
	DSS05.03 Gestionar la seguridad de endpoint.	
	DSS05.04: Gestionar la identidad del usuario y el acceso lógico.	
	DSS05.05 Gestionar el acceso físico a los activos de I&T.	
	DSS05.06: Gestionar documentos sensibles y dispositivos de salida.	
	DSS05.07 Gestionar las vulnerabilidades y monitorizar la infraestructura para detectar eventos relacionados con la seguridad.	
MEA03 — Gestionar el Cumplimiento de los Requisitos Externos	MEA03 — Gestionar el Cumplimiento de los Requisitos Externos.	Procesos. Estructuras Organizativas. Flujos e Información. Personas, Habilidades y Competencias. Políticas y Procedimientos. Cultura, Ética y Comportamiento. Servicios, Infraestructura y Aplicación.
	MEA03.02 Optimizar la respuesta a los requisitos externos.	
	MEA03.03 Confirmar el cumplimiento externo.	
	MEA03.04 Obtener aseguramiento de cumplimiento externo.	

Vigilada Mineducación

Dimensiones	Subdimensiones	Indicadores
Normativa	1581 del 2012. Ley de Protección de Datos Personales.	Cumplimiento.
	1273 del 2009. Ley Delitos Informáticos.	
	2113 del 2021. Funcionamiento de los Consultorios Jurídicos.	

Escriba a continuación ítems y/o componentes que considera que deben ser incluidos o eliminados en el instrumento.

Preguntas que se proponen ser incluidos.	Preguntas que se proponen ser eliminados.

Observaciones:

Hoja 1. Actividades:

- Se debe dejar claro que el nivel 1 es el nivel inicial (Es decir; el nivel en caso de no contar con ese mecanismo)
- Debe quedar claro para el encuestado que es el criterio de Cumplimiento y a que obedecen los 5 Niveles; puesto que se puede confundir pensando que "No cumple" es lo mismo que nivel = 1.

Hoja 2. Estructuras Organizativas:

- Es necesario dejar claridad en estos tres perfiles: Director de TI, Director de Tecnología y Director de Tecnologías Digitales.
- Con respecto al criterio de la casilla SI y NO a que hace referencia, no muestra claridad.

CARGO	SI	NO	CUMPLE SI	CUMPLE NO	OBSERVACION
Director de Riesgos					
Director de TI					
Director de Tecnologia					
Director de Tecnologias Digitales					
Comité de Riesgos Empresariales					
Director de Seguridad de la Informacion					
Dueños del Proceso del Negocio					

Hoja 4. Personas, habilidades y competencias

- Con respecto al criterio de la casilla SI y NO a que hace referencia, no muestra claridad.

PERSONAS, HABILIDADES Y COMPETENCIAS		SI	NO	CUMPLE SI	CUMPLE NO	OBSERVACION
APO12 - Gestionar el Riesgo, APO13 - Gestionar la Seguridad, BAI08 — Gestionar el Conocimiento, DSS05 - Gestionar los Servicios de Seguridad, MEA03 — Gestionar el Cumplimiento de los Requisitos Externos	Gestion de riesgos de negocio.					
	Aseguramiento de la informacion.					
	Gestion de riesgos.					
	Seguridad de la informacion.					
	Desarrollo de la estrategia de seguridad de la informacion.					
	Gestion de la informacion y el conocimiento.					
	Seguridad de la informacion.					
	Gestion de seguridad de la informacion.					
	Pruebas de penetracion.					
	Administracion de seguridad.					

Hoja 5. Políticas y Procedimientos

- Revisar esta tabla porque aparece con el título de la anterior tabla y dejar claridad en los criterios de la casilla SI y NO

PERSONAS, HABILIDADES Y COMPETENCIAS		SI	NO	CUMPLE SI	CUMPLE NO	OBSERVACION
APO12 - Gestionar el Riesgo	Política de riesgo empresarial.					
	Política de riesgo de fraude.					
APO13 - Gestionar la Seguridad	Política de depuración de datos.					
	Política de gestion de datos.					
	Política de evaluacion de la calidad de datos.					
	Política de privacidad.					
BAI08 — Gestionar el Conocimiento	Política de uso del conocimiento sobre gobierno.					
DSS05 - Gestionar los Servicios de Seguridad	Política de seguridad de la informacion.					
MEA03 — Gestionar el Cumplimiento de los Requisitos Externos	Política de cumplimiento.					

- Lo mismo aplica para hojas 6 y 7
- Sería bueno dejar numerada cada hoja del instrumento, solo una recomendación

Se agradece su colaboración para la presente investigación

Apendice D.Encuesta de validación del coeficiente de competencia del experto.

Encuesta para determinar el coeficiente de competencia del experto

Nombres y Apellidos: Claudia Yamile Gómez Llanez

Institución: Universidad Francisco de Paula Santander

Solicitamos a usted muy respetuosamente su colaboración como experto para ser consultado respecto al grado de factibilidad del instrumento para medir la Privacidad de la Información en los Consultorios Jurídicos de las IES. Por tanto, se requiere determinar su coeficiente de competencia en este tema, para esto se requiere la respuesta de las siguientes preguntas de la forma más objetiva que le sea posible.

1.- Marque con una cruz (X), en la tabla siguiente, el valor que se corresponde con el grado de conocimientos que usted posee sobre el tema: "Privacidad de la Información en los Consultorios Jurídicos de las IES". Teniendo en cuenta que según el conocimiento sobre el tema referido va creciendo desde 0 hasta 10.

1	2	3	4	5	6	7	8	9	10
							X		

2.- Realice una auto valoración del grado de influencia de cada una de las fuentes que le presentamos a continuación, según su conocimiento y criterio sobre "Privacidad de la Información en los Consultorios Jurídicos de las IES".

Según la escala tipo Likert marque con una cruz (X), según corresponda, en A (alto), M (medio) o B (bajo).

Fuentes de argumentación	Grado de influencia de las fuentes en sus criterios		
	A (alto)	**M** (medio)	**B** (bajo)
Revisión documental realizada del tema de fuentes nacionales.		X	
Revisión documental realizada del tema de fuentes internacionales.		X	
Experiencia en este campo de estudio.		X	
Su intuición.			

Apendice E.*Cuestionario de Diagnóstico de Privacidad de la Información y Gestión del Conocimiento.*

NIVEL	DESCRIPCION
1	Totalmente en desacuerdo.
2	En desacuerdo.
3	Ni acuerdo ni en desacuerdo.
4	De acuerdo.
5	Totalmente en acuerdo.

Evalúa las siguientes afirmaciones con respecto a tu organización utilizando la siguiente escala:

#	AFIRMACIONES	Totalmente en desacuerdo	En desacuerdo	Ni acuerdo ni en desacuerdo	De acuerdo	Totalmente en acuerdo
1	La organización tiene una política de privacidad de la información claramente definida y comunicada.					
2	Existe un responsable designado para supervisar las cuestiones de privacidad de la información.					
3	Se realizan regularmente evaluaciones y auditorías de riesgos de privacidad.					
4	Se cuenta con un proceso para gestionar y reportar violaciones de privacidad.					
5	La organización sigue un proceso claro para obtener consentimiento antes de recolectar, usar, o divulgar información personal.					
6	Se han implementado controles de acceso para limitar quién puede acceder a la información personal.					
7	Todos los miembros de la organización reciben formación en privacidad de la información.					
8	Existen procedimientos para garantizar la destrucción segura de la información personal que ya no se necesita.					
9	Se gestiona adecuadamente el acceso a la información personal por parte de las personas interesadas.					
10	Se han implementado medidas de seguridad para proteger la información personal.					
11	Se tienen procedimientos claros para responder a las consultas y quejas sobre privacidad.					
12	Se realizan monitorizaciones y revisiones regulares de las prácticas y políticas de privacidad.					
13	La organización dispone de una estrategia clara de gestión del conocimiento.					
14	Existen procedimientos en lugar para recoger y almacenar el conocimiento.					
15	Los miembros de la organización pueden acceder fácilmente al conocimiento cuando lo necesitan.					
16	Se fomenta la creación de conocimiento y la colaboración entre los miembros de la organización.					
17	Se realiza un seguimiento y evaluación regular de las políticas y prácticas de gestión del conocimiento.					

Apendice F.*Evaluación del modelo de privacidad de la información con enfoque en gestión de conocimiento para los consultorios jurídicos de las instituciones de educación superior de Norte de Santander.*

Validación del Modelo

Objetivo: Modelo de privacidad de la información con enfoque en la gestión de conocimiento para los consultorios jurídicos de las instituciones de educación superior de Norte de Santander, el modelo será validado por medio del método Delphi a través de expertos.

Nombre: HUGO FERNANDO CASTRO SILVA **Institución:** UPTC

Nombre del último nivel de escolaridad.		Doctor	
Marque con una **X** el grado de escolaridad con relación a los años de experiencia y cargos que allá tenido.		Tipo de cargo y años de experiencia.	
Grado de Escolaridad		Investigador y/o Docente	Profesional
Profesional			
Licenciado			
Especialista			
Magister			
Doctor	X	25	3
Postdoctoral			

Para optar el título de Magister en Gobierno de TI se presenta la propuesta Modelo de privacidad de la información con enfoque en la gestión de conocimiento para los consultorios jurídicos de las instituciones de educación superior de Norte de Santander, la cual se adjunta para su verificación y posterior valoración.

Por tanto, solicito muy respetuosamente responda la siguiente encuesta teniendo en cuenta las siguientes categorías:

Muy relevante	MR
Bastante relevante	BR
Relevante	R
Poco relevante	PR
No relevante	NR

Marque con una (X) según corresponda.

MODELO DE ACTUACIÓN					
	MR	BR	R	PR	NR
El modelo permite cumplir con el objetivo propuesto.	x				
El modelo se sustenta en estándares reconocidos y normativas vigentes.	x				
Existe pertinencia en los elementos incorporados en el modelo.	x				
El modelo podría ser adaptado a un consultorio jurídico de una IES.	x				

Escriba a continuación que fases y/o componentes considera que deben ser incluidos o eliminados/modificados en este modelo.

Fases y/o componentes que se proponen ser incluidos.	**Fases y/o componentes que se proponen ser eliminados/modificados.**
Diagnóstico de privacidad de la información? O Mejora continua?	No es claro en el modelo el instrumento al final del mismo de que fase hace parte
Monitoreo y revisión continua	Se puede indicar cuales KPIs pueden ser aplicables

Señale a continuación, si considera que el nombre de alguno de los ítems del modelo debe ser cambiado.

La fase y/o componente aparece como.	**La fase y/o componentes debe ser cambiado por.**

Se agradece su colaboración para la presente investigación

Apendice G. *Certificado de participación al X Congreso Internacional Dossier 2024.*



Universidad Francisco De Paula Santander Ocaña y la Facultad de Ciencias Administrativas y Económicas

Certifican que:

Yan Carlos Angarita Sanguino

CC 1091661138

Participó como ponente

X Congreso Internacional Dossier 2024

III Coloquio Internacional de Investigación

"50 Años impulsando la innovación: inteligencia artificial y transformación de ideas en valor empresarial"

En la Universidad, los días 04 al 06 de Junio de 2024

Tema: Gestión del Conocimiento para los Consultorios Jurídicos de las Instituciones de Educación Superior

Wilder Quintero Quintero
Decano (E.) Facultad de Ciencias Administrativas y Económicas

Leidy Torcoroma Guerrero Prado
Directora del Centro de Investigación para el Desarrollo Regional [CIDER]