UNIVERSIDAD PERUANA UNIÓN

ESCUELA DE POSGRADO

Unidad de Posgrado de Ingeniería y Arquitectura

Diseño de un sistema automatizado de gestión de la seguridad de la información basado en la Norma ISO/IEC 27001:2013 para dar cumplimiento a la Ley 1581 de 2012 de protección de datos personales en el departamento de sistemas de una institución universitaria en Colombia

Tesis para obtener el Grado Académico de Maestro en Ingeniería de Sistemas con Mención en Dirección y Gestión en Tecnología de información

Autor:

Javier Francisco Córdoba Perdomo

Asesor:

Mg. Fernando Manuel Asin Gómez

Lima, julio de 2021

ANEXO 07 DECLARACIÓN JURADA DE AUTORÍA DEL INFORME DE TESIS

Mg. Fernando Manuel Asin Gómez

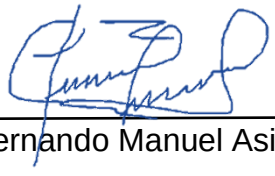
Asesor de la Escuela de Posgrado, Unidad de Posgrado de Ingeniería y Arquitectura, de la Universidad Peruana Unión.

DECLARO:

Que el presente informe de investigación titulado: ***"Diseño de un sistema automatizado de gestión de la seguridad de la información basado en la Norma ISO/IEC 27001:2013 para dar cumplimiento a la Ley 1581 de 2012 de protección de datos personales en el departamento de sistemas de una institución universitaria en Colombia"*** constituye la memoria que presenta el **Bachiller Javier Francisco Córdoba Perdomo** para aspirar al título al Grado académico de **Maestro en Ingeniería de Sistemas con Mención en Dirección y Gestión en Tecnología de información** ha sido realizada en la Universidad Peruana Unión bajo mi dirección.

Las opiniones y declaraciones en este informe son de entera responsabilidad del autor, sin comprometer a la institución.

Y estando de acuerdo, firmo la presente constancia en *Lima,* el 2 de julio del año 2021



Mg. Fernando Manuel Asin Gomez

ACTA DE SUSTENTACIÓN DE TESIS DE MAESTRO(A) 315

En Lima, Ñaña, Villa Unión, a 02 días del mes de julio del año 2021, siendo las 10:00 a. m, se reunieron en la modalidad online sincrónica, bajo la dirección del Señor Presidente del Jurado: Dr. Josué Edison Turpo Chaparro, el secretario: Mg. Sergio Omar Valladares Castillo, los demás miembros: Dra. Erika Inés Acuña Salinas, Mg. Nemias Saboya Ríos y el M.Sc. Fredy Abel Huanca Torres y el asesor: Mg. Fernando Asin Gomez, con el propósito de administrar el acto académico de sustentación de Tesis de Maestro(a) titulada: Diseño de un sistema automatizado de gestión de la seguridad de la información basado en la Norma ISO/IEC 27001:2013 para dar cumplimiento a la Ley 1581 de 2012 de protección de datos personales en el departamento de sistemas de una institución universitaria en Colombia del Bachiller/Licenciado(a) Javier Francisco Córdoba Perdomo

Conducente a la obtención del Grado Académico de Maestro(a) en: Ingeniería de Sistemas

(Nomenclatura del Grado Académico)

con Mención en Dirección y Gestión de Tecnologías de Información. El Presidente inició el acto académico de sustentación invitando al candidato hacer uso del tiempo determinado para su exposición. Concluida la exposición, el Presidente invitó a los demás miembros del Jurado a efectuar las preguntas, cuestionamientos y aclaraciones pertinentes, los cuales fueron absueltos por el candidato. Luego se produjo un receso para las deliberaciones y la emisión del dictamen del Jurado.

Posteriormente, el Jurado procedió a dejar constancia escrita sobre la evaluación en la presente acta, con el dictamen siguiente:

Bachiller/Licenciado (a): Javier Francisco Córdoba Perdomo

CALIFICACIÓN	ESCALAS			Mérito
	Vigesimal	Literal	Cualitativa	
APROBADO	16	B	Con nominación de bueno	Muy bueno

(*) Ver parte posterior

Finalmente, el Presidente del Jurado invitó al candidato a ponerse de pie, para recibir la evaluación final. Además, el Presidente del Jurado concluyó el acto académico de sustentación, procediéndose a registrar las firmas respectivas.

Presidente | Secretario

Asesor | Miembro | Miembro

Bachiller/Licenciado(a)

DEDICATORIA

A Dios quien da la inteligencia y la sabiduría.

A mi amada esposa Elizabeth.

A mis queridos hijos Juan, Javier y Miguel.

A mis queridas madre Reinelda y hermana Milena.

A mi apreciada Corporación Universitaria Adventista UNAC.

AGRADECIMIENTOS

A Dios, porque sus planes son mejores que los míos, porque me da sabiduría para desarrollar todos los proyectos, en especial este de formación académica, porque me capacita para servir mejor a su Iglesia y a la sociedad.

A mi familia, por el apoyo, por la paciencia y el tiempo que me dieron para desarrollar mi formación de postgrado.

A la Corporación Universitaria Adventista UNAC, por el apoyo financiero y la oportunidad de aplicar los conocimientos adquiridos en el Departamento de Sistemas.

A la Universidad Peruana Unión, porque a través de sus profesores y personal administrativo, su formación académica y formación en valores que me han permitido acercarme más a Dios, ha sido la casa de estudio que me ha permitido lograr un objetivo más en mi crecimiento profesional.

A mis compañeros de trabajo en el Departamento de Sistemas, porque han sido parte activa en el desarrollo de esta tesis al apoyarme con sus conocimientos en cada una de sus áreas, Desarrollo de Software, Conectividad e Infraestructura TIC.

Al Mg. Fernando Manuel Asin Gómez, quien como asesor en la Universidad Peruana Unión me apoyó durante el desarrollo de la tesis. A la Mg. Jennifer Lemos, quien me orientó para que la tesis lograra su objetivo y a todos los que contribuyeron para que este trabajo cumpliera con lo propuesto.

TABLA DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

SÍMBOLOS USADOS

UNAC: Corporación Universitaria Adventista

DSI: Departamento de Sistemas e Informática

ISO: Organización Internacional para la Estandarización

IEC: Comisión Electrotécnica Internacional

SGSI: Sistema de Gestión de la Seguridad de la Información

PHVA: Planear, Hacer, Verificar y Actuar

RNBD: Registro Nacional de Bases de Datos

TIC: Tecnología de la Información y la Comunicación

MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

ITI: Biblioteca de infraestructura de tecnología de la información

SAP-LAP: Situación, Actor, Proceso-Aprendizaje, Acción, Desempeño

INCIBE: Instituto Nacional de Ciberseguridad

RESUMEN

La gestión de la seguridad de la información es una apuesta inevitable en toda organización, tanto por la gestión interna del activo más importante, la información, que representa en términos de datos y conocimiento, como para responder a las disposiciones legales que para el caso de la protección de datos personales en Colombia se regulan mediante la Ley 1581. En este sentido, la presente investigación tiene como objetivo diseñar un Sistema de Gestión de la Seguridad de la Información basado en la Norma ISO 27001:2013 para El Departamento de Sistemas que cumpla con los requisitos que exige el gobierno colombiano a través de la Ley 1581 de 2012 para la protección de datos personales. Para ello se propone una investigación aplicada con enfoque tecnológico que se apoya del software Eramba Community para ofrecer una alternativa de implantación del sistema a bajo costo. Dentro de los resultados se encontró que el Departamento de Sistemas de la institución universitaria no daba cumplimiento a la Ley 1581, pese a sus esfuerzos por intentar sin suficiente rigor responder a ella desde procedimientos manuales, oportunidad que sirvió de punto de partida para proponer un SGSI automatizado para responder con el marco legal con apoyo de la Norma ISO 27001. Se concluye que la mirada sistémica incluida en integración de la Norma ISO 27001:2013 para dar respuesta a la Ley de protección de datos personales mediante un software libre resultó un procedimiento eficiente, ya que permitió el cumplimiento ágil de los procedimientos como es natural en toda tarea automatizada, sin exceder recursos presupuestales de la Universidad y mejora la seguridad de los procesos.

Palabras clave: SGSI, ISO 27001:2013, Ley 1581 de 2012, datos personales, Eramba Community

ABSTRACT

The management of information security is an inevitable bet in any organization, both for the internal management of the most important asset, information, which represents in terms of data and knowledge, and to respond to the legal provisions that in the case of personal data protection in Colombia are regulated by Law 1581. In this sense, the present research aims to design an Information Security Management System based on the ISO 27001:2013 Standard for The Systems Department that meets the requirements demanded by the Colombian government through Law 1581 of 2012 for the protection of personal data. For this purpose, an applied research is proposed with a technological approach that is supported by Eramba Community software to offer an alternative for the implementation of the system at low cost. Among the results it was found that the Systems Department of the university institution did not comply with Law 1581, despite its efforts to try without sufficient rigor to respond to it from manual procedures, an opportunity that served as a starting point to propose an automated ISMS to respond to the legal framework with the support of ISO 27001. It is concluded that the systemic view included in the integration of the ISO 27001:2013 Standard to respond to the Personal Data Protection Law through free software was an efficient procedure, since it allowed the agile compliance of procedures as is natural in any automated task, without exceeding the University's budgetary resources and improving the security of the processes.

Keywords: ISMS, ISO 27001:2013, Law 1581 of 2012, personal data, Eramba Community

CAPÍTULO I. PROBLEMA DE INVESTIGACIÓN

Con el auge y crecimiento de las Tecnologías de Información y Telecomunicación (TIC), la gestión, almacenamiento, conservación y de los datos se ha vuelto esencial para las organizaciones en la medida en que representan un activo y una ventaja sobre la competencia. En esta medida, son muchos los esfuerzos por parte de las organizaciones para hacer frente a las vulneraciones relacionadas por ejemplo con el robo o secuestro de información, donde las medidas de seguridad son efectivas en cierto grado para reducir las consecuencias de riesgos tales.

Sin embargo, así como las empresas deben actuar en protección frente a sucesos que vulneren su sistema de información, también están obligadas por Ley a proteger los datos personales de clientes y usuarios que incluyan en sus bases de datos, en tanto, la exposición de los mismos podría afectar su vida íntima. De ahí que el desacato a dicha directriz pueda poner en riesgo financiero a las organizaciones, ya que el incumplimiento es sancionado con multas.

En Colombia, la Ley que orienta la protección de datos personales es la 1581 de 2012, la cual como ya se menciono es de obligatorio cumplimiento por toda organización a nivel nacional. Sin embargo, en este ámbito existe también la Norma

internacional ISO 27001:2013 que sin ser obligatoria es un complemento ideal para la Ley, ya que proporciona orden a todo el proceso de la seguridad de la información desde un enfoque integrado. De esta manera, siguiendo el caso de la institución universitaria de estudio y otros trabajos desarrollados en la misma línea, con el fin de optimizar los procesos organizacionales en esta materia, ha sido pertinente la articulación de la Ley con la Norma cuando esta contribuye a mejorar los procesos de seguridad de la información.

En tal posibilidad, la articulación se ha venido dando de manera manual y empiezan a aparecer propuestas de automatización mediante software (Arévalo, Bayona y Rico, 2015; Giraldo, 2016; Montesino, Baluja y Porvén, 2013; Valencia y Orozco, 2017), que permiten mayor orden y agilidad en el cumplimiento. Conforme a este panorama la presente investigación se propone diseñar un sistema automatizado de gestión de la seguridad de la información basado en la Norma ISO/IEC 27001:2013 para dar cumplimiento a la Ley 1581 de 2012 de protección de datos personales en el Departamento de Sistemas de una institución universitaria en Colombia, reconociendo que dicho esfuerzo busca llevarse a cabo como una propuesta de bajo presupuesto ajustándose a los recursos de que dispone la institución de estudio.

De esta manera, el documento presenta cinco capítulos. El primer capítulo ofrece un contexto sobre el problema, los argumentos que lo justifican, los objetivos e hipótesis. El capítulo dos ofrece el sustento teórico, empírico y legal. El capítulo tres da cuenta de la propuesta metodológica. El capítulo cuatro de la gestión del proyecto en tanto su planificación que los requerimientos, incluye los alcances, limitaciones y recursos, para terminar con el capítulo cinco donde se presentan los resultados, la discusión, las conclusiones y recomendaciones del proceso de investigación.

1.1 Identificación del problema

En la actual era del conocimiento, la información generada por las organizaciones se convierte en el principal activo de estas, por tanto, su disponibilidad y seguridad se convierten en los pilares fundamentales para el éxito o fracaso de los negocios o de los objetivos institucionales, lo que exige mayor sensibilización sobre el tema entre directivos y operativos para que se reduzca la oportunidad de riesgos y la exposición a los ataques que pueden resultar en la modificación hasta el robo de la información [1].

En este sentido, los avances tecnológicos de la última década como los equipos móviles y de cómputo utilizados para el procesamiento, almacenamiento y transmisión de información, tanto para fines personales como profesionales, han llegado a niveles inimaginables que exigen retos importantes a nivel de la seguridad de esta. Se podría decir que conforme avanza la tecnología se incrementan los niveles y los distintos tipos de riesgos en contra de la protección de la información, ya que cada vez son más complejos los métodos a través de los cuales se intenta acceder de manera ilegal a los sistemas de información [2].

De acuerdo con el contexto anterior, si bien, todas las organizaciones independientemente de su naturaleza pueden estar expuestas a vulnerabilidades, la firma de abogados Marrugo Rivera y Asociados señala que el sector Educativo presenta mayor vulnerabilidad ya que tradicionalmente ha sido uno de los más descuidados en estos asuntos [25]. Es preocupante este diagnóstico en el caso de las universidades públicas y privadas, si se tiene en cuenta el riesgo en cuanto al registro y modificación de notas de miles de estudiantes durante cada semestre, por

no mencionar aspectos que redunda en información de nuevo conocimiento o patentes.

En Colombia, por ejemplo, se han documentado los casos de la Universidad del Tolima la cual sufrió un ataque informático en el año 2018, en el que se modificaron las notas de más de 18.000 estudiantes; y el caso de la Universidad Mariana de la ciudad de Pasto, caso más preocupante aún, pues las autoridades lograron identificar una especie de mercado de notas en el que se pedían hasta dos millones de pesos por la modificación de las notas parciales y finales [25].

Estos casos llevan a considerar las medidas establecidas por el gobierno colombiano con el fin de mitigar este tipo de riesgos y de mejorar la competitividad de las organizaciones. Frente a lo cual, tras la firma de varios tratados comerciales[1], Colombia ha creado un marco legal a través de la Ley 1581 de 2012, que obliga a las organizaciones a proteger su hardware, software e información con una gestión organizada y procesos claramente definidos [3].

Esta Ley también es conocida como la Ley de Protección de Datos Personales, la cual reconoce y protege el derecho que tienen todos los ciudadanos colombianos a saber, poner al día y corregir las informaciones que estén registradas en las bases de datos o archivos de cualquier organización pública o privada [4].

De manera específica, mediante el capítulo 26 del Decreto Único 1074 de 2015, el gobierno colombiano dio los lineamientos para registrar las bases de datos que se administran en el RNBD. El Registro Nacional de Bases de Datos es el repositorio público de las bases de datos que los ciudadanos pueden revisar de manera libre y que se administra por la Superintendencia de Industria y Comercio. [5].

[1] Entre ellos, con la Unión Europea en el año 2013.

Complementariamente, pero desde el ámbito internacional, la Norma ISO/IEC 27001:2013 se presenta como una herramienta de gestión estratégica que ayuda a proteger la información independientemente de la voluntad de la organización por certificar o no su sistema de gestión de la seguridad, considerando, sobre todo, que lo importante es aplicar buenas prácticas en sus procesos internos y externos, como lo asegura [6].

Conforme al panorama anterior, se reconoce la necesidad de proteger la información como activo clave dentro de las organizaciones, a partir de las leyes y normas que a nivel nacional e internacional respaldan tal hecho. A partir de esta consideración se observa el contexto de estudio, el cual remite a una institución de educación superior.

La problemática se visualiza al encontrar, por un lado, que la institución carece de un SGSI basado en la Norma ISO/IEC 27001:2013, ya que lo que existe es un conjunto de procedimientos internos que se gestionan de manera manual y fueron creados de manera autónoma por el Departamento de Sistemas de la institución universitaria para dar respuesta a la necesidad de protección de la información.

Se asume en este sentido, que la no formalización de la Norma tiene que ver con el carácter no obligatorio para llevar a cabo su implementación, lo que ha hecho que hasta el momento no fuera una prioridad para la institución, aun cuando reconoce su importante aporte a la organización y mejoramiento continuo de los procesos. Dato que se convierte en una opción estratégica para la dirección del Departamento en mención quien tiene considerada su implementación independiente de la certificación, ya que no es imperativo realizarla [7].

Por otro lado, en cuanto a la Ley, si bien se ha venido cumpliendo con el RNBD ante la entidad competente, se observa que la respuesta a dicho requisito puede mejorarse si se articula con los procedimientos de organización de información que ofrece la Norma. Aún más, se puede lograr más eficacia si tanto la Norma como la integración de la Ley pueden operar de manera automatizada atendiendo a la naturaleza del Departamento de Sistemas que busca poner en marcha la propuesta.

De esta manera, se está dando una mejora en la seguridad de la información pasando de procedimientos manuales y sin estándares de calidad, a procedimientos automatizados que permite un cumplimiento a las disposiciones legales de manejo de la información en Colombia mediante criterios internacionales. Por tanto, la problemática actual radica en la falta de agilidad en la gestión de la seguridad que representa una operación manual de la información para responder a los requerimientos de la Ley en mención, lo que incrementa el riesgo de vulnerabilidades tanto tecnológicas como legales y financieras.

En síntesis, queda claro que el mundo está ante nuevas y constantes oportunidades generadas por los avances tecnológicos actuales y por venir, los cuales dan lugar a nuevos riesgos en la gestión de la información, por lo cual, para la Universidad se hace imprescindible que los procedimientos se tornen cada vez más ágiles en la medida en que permiten responder con sus objetivos propuestos en el interés de ofrecer calidad y satisfacción a sus clientes, reduciendo los riesgos de vulnerabilidad.

1.2 Justificación

La propuesta de diseñar un Sistema de Gestión de la Seguridad de la Información -SGSI- basado en la Norma ISO/IEC 27001:2013 inicialmente responde a la necesidad de organización de los procesos internos del Departamento de Sistemas en una institución universitaria con el fin de estandarizarlos, hacerlos más eficaces y eficientes de tal manera que garantice el almacenamiento y salvaguarda de la información.

En este sentido, la Normativa ISO es una propuesta externa independiente para el mejoramiento continuo de los procesos de las organizaciones en pro de la calidad y la producción o prestación de servicios, sin embargo, de ninguna manera se presenta en un marco de implementación obligatoria, no obstante, puede afirmarse que una vez se reconoce la estructura de la Norma, para el caso la ISO/IEC 27001:2013, se logra considerar que sus elementos constituyentes aportan al desarrollo las actividades operativas proyectadas por una organización. En esta medida, insertar la lógica de trabajo que propone la Norma a los procesos internos, tampoco exige la certificación en la misma, pero brinda un valor agregado a la prestación del servicio e incluso posibilita las bases para la formalización futura de la implementación de la Norma en caso la institución universitaria lo decida [7].

De la misma forma, la Norma tampoco exige la automatización de su propuesta de calidad, aunque algunos procesos, por decisión interna de las organizaciones, exigen el procesamiento de la información de manera digital y automatizada. Sin embargo, considerando la naturaleza del departamento de la universidad donde se quiere diseñar el SGSI y para efectos de agilizar los procesos, se busca que la estructura del sistema de gestión migre hacia un nivel tecnológico aprovechando los recursos disponibles en la organización, sin generar una destinación presupuestal adicional.

Ahora, luego de justificar el interés acerca de la incorporación de la Norma de manera automatizada al Departamento de Sistemas de la institución de estudio para efectos de aportar a la calidad en la gestión y seguridad de la información, así como a la agilización del dicho procedimiento requerido en esta línea, el informe de investigación se propone articular esfuerzos permitiendo que la incorporación de tal sistema contribuya al cumplimiento de la Ley 1581 de 2012 de Protección de Datos Personales, la cual no es de carácter voluntaria sino obligatoria. Así, se contribuye con la optimización de los procesos y se cumple con la Ley, la cual es de estricto cumplimiento para todas las organizaciones independiente de su objeto social.

Para el caso específico de las instituciones universitarias, la Ley 1581 de 2012 adquiere una importancia especial considerando que los programas académicos deben tener registro calificado para ser ofrecidos y desde el 25 de julio de 2019 el Decreto 1330 mediante el Artículo 2.5.3.2.11 Protección de datos, exige que:

> Tanto el Ministerio de Educación Nacional, como las instituciones deberán implementar todos los protocolos y garantías del derecho a la protección datos personales según lo dispuesto en la Ley 1581 2012 en la cual se dictan disposiciones generales para la protección datos personales o la Norma que la modifique, sustituya o derogue, como las Normas que la desarrollen y complementen [8].

En caso de tener conocimiento posibles vulneraciones a dicho derecho, los hechos deberán ser puestos en conocimiento de la autoridad competente [8]. Esta nueva disposición legal valida la pertinencia de la propuesta en el contexto de estudio y la necesidad de incorporarse en los alcances de la investigación para efectos del trabajo degrado que exige la maestría. Así mismo, en un sentido práctico, se

contribuye a generar valor agregado a los procesos de una organización mediante procedimientos que proporcionen eficiencia y eficacia en las actividades.

Por su parte, cuando se hace referencia a la automatización del cumplimiento legal frente a la seguridad de la información mediante estándares de calidad, implica la utilización de medios tecnológicos que pueden incrementar el presupuesto de las organizaciones que decidan implementar la propuesta que aquí se realizan. No obstante, el medio tecnológico que para el caso es el software Eramba, representa un recurso clave para automatizar un proceso. Al ser de código abierto disminuye los costos y permite adaptarse tanto a la norma como a las leyes y a los procesos de las organizaciones.

En este sentido, el aporte a las instituciones de educación superior, contexto en el cual se consideró la implementación de la propuesta, o cualquier organización que desee adoptarla como un punto de partida, se verá reflejado en una baja inversión y en la respuesta oportuna y ágil frente a las exigencias legales que buscan mejorar al interior de las organizaciones la gestión de la seguridad de la información.

1.3 Objetivos

1.3.1 Objetivo general

Diseñar un sistema automatizado de gestión de la seguridad de la información basado en la Norma ISO/IEC 27001:2013 para dar cumplimiento a la Ley 1581 de

2012 de protección de datos personales en el Departamento de Sistemas de una institución universitaria en Colombia.

1.3.2 Objetivos específicos

- Realizar un diagnóstico sobre los procedimientos adelantados por el Departamento de Sistemas para la gestión de la seguridad de la información en la institución universitaria de estudio alineados a la Norma ISO/IEC 27001:2013 y la Ley 1581 de 2012.
- Diseñar un sistema que integre los requisitos de la Norma ISO/IEC 27001:2013 con las exigencias impuestas por la Ley 1581 de 2012 de protección de datos personales en Colombia.
- Automatizar un sistema de seguridad de la información basado en la ISO/IEC 27001:2013 con la herramienta tecnológica de código abierto Eramba Community para que dé cumplimiento a la Ley 1581 de 2012.
- Evaluar el funcionamiento del sistema automatizado de seguridad de la información basado en la ISO/IEC 27001:2013 y la Ley 1581 de 2012.

CAPÍTULO II. MARCO TEÓRICO

2.1 Antecedentes de la Investigación

En el presente apartado se relacionan los estudios previos relacionados con el objeto de estudio organizados en tres subtítulos con investigaciones que hacen referencia a los sistemas de gestión de seguridad de la información, protección de datos personales y automatización del sistema de gestión de información.

2.1.1 Sistema de Gestión de Seguridad de la Información basados en la Norma ISO/IEC 27001

La bibliografía recuperada para la construcción de antecedentes presenta una ventana de observación de 11 años, con información respectiva a la Norma ISO 27001, la Protección de Datos y su Normativa en Colombia y la automatización del SGSI.

Sobre la Norma ISO 27001, según las búsquedas realizadas para este trabajo, se recuperan documentos desde 2008 al 2019, que hacen referencia a las políticas para la seguridad de la información basadas en la Norma, análisis del riesgos de la información, el diseño, la implementación del Sistema de Gestión de Seguridad de la Información -SGSI-, dentro de la cual aparecen estudios sobre análisis previos, metodologías, requisitos, cumplimiento, controles de seguridad, el presupuesto requerido, la opción de contratar un consultor externo para su implementación y la evaluación tras la incorporación del sistema.

Amparado en la Norma ISO 27001 Velasco [6] en su documento titulado “El derecho informático y la gestión de la seguridad de la información una perspectiva con base en la norma ISO 27001”, ofrece una perspectiva del Derecho Informático y de la Gestión de la seguridad de la información para concientizar acerca de la

necesidad de establecer políticas de seguridad de la información en las organizaciones, independiente de la ausencia, para entonces, de una reglamentación nacional, ya que las Normas internacionales han ofrecido un adecuado soporte para garantizar la protección de la información. La metodología que implementó el autor para dar cuenta de las áreas de impacto en la gestión de la información remite al componente del cumplimiento de la norma ISO 27001. El autor concluye diciendo que la Norma ISO/NTC 27001 no es más que el agente regulador para la reglamentación y autorregulación en las organizaciones ya que imparte las reglas y parámetros necesarios en la gestión de sus activos de información siguiendo los debidos protocolos de seguridad. Esta referencia resulta particularmente importante para el presente estudio, ya que el interés por proteger la información, si bien emerge por requerimiento de Ley, busca soportarse en la Norma internacional ISO 27001 para ordenar los procesos internos de protección de información, sin establecer el compromiso de certificación.

En la misma dirección, De Freitas [26], en su investigación titulada “Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar”. En el estudio, la autora se propone identificar las fortalezas y debilidades a los que estaban expuestos los activos de información que tiene en custodia de la institución, para plantear sugerencias a los posibles ataques que puede presentar la información de la institución haciéndola vulnerable. La metodología se basa en un estudio de caso, que permitió la recolección de datos mediante entrevistas semi-estructuradas, estructuradas y en profundidad, revisión bibliográfica y arqueo de fuentes, complementario a un estudio in-situ en las instalaciones del contexto de estudio para identificarlos aspectos de seguridad física previstos en las Normas ISO-27001:2007. La conclusión reconoce la importancia que tiene la información reservada por la

Universidad y sugiere la aplicación de algunos controles que establece la norma ISO para dicho activo. Para el caso de la institución de estudio, además de la protección de los datos, la información relevante es de carácter académico y administrativo y la ausencia de un sistema de gestión de seguridad basado en la Norma ISO/IEC 270001 se presenta entonces como un riesgo, ya que su implementación aporta también a la minimización de los riesgos en una lógica mejora continua.

En el mismo sentido de los riesgos que presenta la información, Caviedes y Prado [27] en su estudio “Modelo unificado para identificación y valoración de los riesgos de los activos de información en una organización” se proponen desarrollar un modelo unificado para la identificación y valoración de los riesgos de la información dentro de un sistema de seguridad de la información para cualquier contexto organizativo. El modelo constituye una herramienta que permita agilizar los procesos, intuitiva y alineada con las recomendaciones ofrecidas por los entes de control durante las auditorias, en la medida en que se están protegiendo los activos de información de las amenazas que ponen en riesgo la misma. Este aporte de los autores se alinea con los propósitos de la presente investigación en tanto se busca, aunque con una intencionalidad diferente, una articulación de la Ley de Protección de Datos personales con el diseño del SGSI, que también es objeto de estudio para la investigación en curso desde la automatización.

Otro trabajo que plantea un análisis de riesgo de información lo presenta Giraldo [22], titulado “Análisis para la implementación de un sistema de gestión de seguridad de la información según la norma ISO 27001 en la empresa Servidoc S.A.” realiza un análisis previo a la implementación de un sistema de gestión de seguridad de la información ISO 27001, para proponer soluciones de seguridad informática en las áreas críticas donde las vulneraciones pueden tener mayores implicaciones como en

áreas de Contabilidad, Facturación e Historias Clínicas. Se concluyó que un análisis previo permite las bases para la implementación del sistema de Gestión de Seguridad de la Información bajo la norma ISO/IEC 27001:2013 y así mismo permite la delimitación de soluciones de seguridad. Para el caso presente en el contexto de una institución universitaria, un análisis previo permite la información que requiere mayor cuidado corresponde a la financiera y académica la cual se administra desde el Departamento de Sistemas.

Advisera Expert Solution en el mismo año, publican tres artículos orientados a reflexionar sobre la privacidad y la seguridad cibernética a partir de la ISO 27001 [29], la planeación del presupuesto que se requiere para implementar dicha Norma [28] y la comparación entre una implementación desde el enfoque del consultor y el enfoque "hazlo tú mismo" [30].

En el primer caso "Privacy cyber security and ISO 27001" [29], el artículo presenta la evolución acerca de la protección de la información tras la preocupación por la privacidad, la cual ha estado marcada según cada momento histórico. Metodológicamente se identifican las variables que distinguen la preocupación individual por la privacidad o la protección de información, de la preocupación que puede ocurrir en el marco de una organización, ya que sus niveles de riesgo son diferenciados, reconociendo la importancia de tres factores clave: cuándo, cómo y hasta qué punto se comunican los datos y la información. Se concluye que, sin excluir la integración de sistemas de seguridad y privacidad a usuarios individuales, los sistemas de seguridad se recomiendan para las organizaciones públicas y privadas por lo que implica los costos en relación con el volumen de datos que requieren proteger. Ahora, al hablar de costos, se pone de manifiesto el tema presupuestal requerido en un proyecto que pretenda aplicar la Norma ISO 27001. Si bien, el SGSI

se ha establecido como una herramienta para apoyar los procesos organizativos en pro de asegurar la información, a costos optimizados y con resultados previstos, los esfuerzos que se puedan emprender dentro del plazo del proyecto pueden llegar a ser inútiles.

El segundo documento de Advisera Express Solution titulado “How to Budget an ISO 27001 Implementation Project” [28], plantea las implicaciones de la implementación de un SGSI, ya que, en la medida que se presenta como herramienta de apoyo organizativo para mantener protegida la información, plantea una forma optimizada para gestionar los costos y permite la obtención de los resultados previstos conforme al esquema organizativo de la norma. Se concluye que este aspecto resulta importante, ya que de no posibilitarse dichos resultados los esfuerzos serían inútiles si los costos de implementación exceden los beneficios.

Otro artículo de Advisera Express Solution “Implementing ISO 27001 with a consultant vs . DIY approach” [30] plantea la reflexión entre contratar un consultor externo o llevar a cabo las acciones internamente desde la empresa. El análisis indica que en el primer caso no siempre se generan los mayores beneficios en cuanto a costos e imagen de la empresa para atender a las disposiciones legales. Se concluye que es posible una gestión interna de la información que garantice su seguridad y para ello se cuenta con el sistema de gestión estandarizado procedente de la norma ISO 27001. Reflexión apropiada para efectos de la presente investigación, que internamente se organiza para responder con la Ley 1581 de 2012 de protección de datos personales en Colombia.

Por su parte, Valencia y Orozco [24] proponen una metodología para la implementación de un sistema de gestión de seguridad de la información (SGSI) de acuerdo con todo el conglomerado de Normas que abarca la ISO/IEC 27000 en torno

a las actividades requeridas para cumplir con los requisitos de la ISO/IEC 27001, los controles de seguridad de la ISO/IEC27002, esquemas de riesgos de la ISO/IEC 27005 y las recomendaciones de la ISO/IEC 27/003. La metodología que propuso esta investigación estuvo articulada por cinco fases que permitieron un desarrollo tanto conceptual como metodológico de la propuesta y que incluyó personas, tiempos y recursos entre los que se encuentra el respaldo de la Alta Dirección para el cumplimiento de los objetivos. En su conjunto, estas Normas permitieron la implementación de un SGSI, sin embargo, los autores ponen de manifiesto la complejidad con la cual se desarrolla el proceso de desarrollo del sistema completo.

Saliéndose de la propuesta de la implementación del SGSI Ahman, Hendy y Abba [31] en su investigación titulada “Evaluation of ISO 27001 implementation towards information security of cloud service customer in PT. IndoDev Niaga Internet” proponen una evaluación tras la implementación de la ISO 27001:2013 para saber hasta qué punto se ha aplicado el proceso y qué acciones se pueden realizar para mejorar el rendimiento de la aplicación de la norma ISO 27001: 2013. En primer lugar, se realizó un análisis factorial para determinar los factores que afectan a la seguridad de la información. Una vez conocidos los factores que afectan a la seguridad de la información, se realizaron observaciones y entrevistas para recopilar datos sobre PT. En esta evaluación los autores encuentran que el factor más influyente para la seguridad del cliente en el contexto de estudio es el control de acceso donde se encontraron que de 33 elementos de control 11 estuvieron en la categoría de no conformidad y en las operaciones de seguridad se encontró que de los 12 controles 5 presentan no conformidad.

Cares y Diéguez [32] en su trabajo “Comparación de dos enfoques cuantitativos para seleccionar controles de seguridad de la información” se interesaron en comparar dos enfoques cuantitativos para seleccionar controles de seguridad de la información que apoyaran la toma de decisiones sobre inversiones de seguridad cuando se presenta restricciones presupuestarias. El primer enfoque es de programación de conjuntos de respuesta -ASP- y el segundo programación lineal -PL-. El primero se presenta adecuado para unos pocos controles que facilitan la etapa de modelado debido al alto nivel de abstracciones de su lenguaje de programación. El segundo, basado en PL, presenta un excelente rendimiento, aunque su formulación algebraica resulta un poco más compleja de especificar que ASP. Estos aportes resultan particularmente importantes porque coinciden con la propuesta de implementación el SGSI con restricciones presupuestarias y aunque no se pretende ahondar en los controles de seguridad, si permite confirmar que la automatización del proceso de seguridad de la información puede llevarse a bajo costo si se implementan por ejemplo herramientas de código abierto frente a herramientas de paga.

Por último, en esta línea Amogh y Jayshree [33] con el estudio “Best practices of auditing in an organization using ISO 27001 standard” hacen énfasis en las ventajas competitivas que trae la certificación ISO 27001 a una organización y en general el conjunto que compone la ISO/27000. Para ello, los autores estudiaron la norma ISO 27001 e implementaron el marco ISO 27001 de acuerdo con los requisitos de la organización de estudio. Junto con esto, también analizaron las diferentes políticas que se aplican en la organización, lo que les ayudó para que la empresa se protegiera de las amenazas a la seguridad, ayudándole así mismo a aumentar su productividad. Concluyen que la seguridad de la información cada vez se está convirtiendo en una preocupación pública, lo que convierte a la norma ISO 27001 un tema actual y

actuante que proporciona ventajas competitivas. Agregan los autores que los problemas presentes en una organización en términos de seguridad de la información pueden ser contrarrestados mediante la implementación de la norma en mención.

2.1.2 Protección de Datos Personales

El primer documento que se referencia sobre el tema de la protección de los datos personales pertenece a Ribagorda [34] y fue titulado “La protección de datos personales y la seguridad de la información” cuyo objetivo se orienta a establecer la relación entre la protección y los requisitos de seguridad de la información que se proporcionar para su cumplimiento desde la Norma ISO /IEC 27001. A nivel metodológico se especifican los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la información. El autor concluye que la protección de datos personales solo puede ser satisfecha si se siguen las consideraciones de índole administrativo y organizativo. De esta manera, se puede acceder al derecho para garantizarlo y brindar los elementos de confianza a la sociedad usuaria de las tecnologías de la información.

Sobre protección de datos personales, Alcalde, Zeidler, Klein, Cornel, Fernandez, Matias [35] en su documento titulado “Enabling personal privacy for pervasive computing environments” los autores presentan una arquitectura novedosa que amplía el control de la privacidad de forma subestatal y complementa la privacidad empresarial con la incorporación de la privacidad personal. La metodología propone un modelo holístico de protección de la privacidad en entornos empresariales que también protegen la privacidad personal a partir del desafío que representa las políticas para navegar en internet. Se concluye que, dado el reto que representa la

protección de datos en la actualidad, los usuarios tienen un papel activo en la toma de decisiones respecto de aceptar las condiciones de las políticas de privacidad que establece cada sitio web, luego si tiene mayores elementos para tomar estas decisiones, están aportando a la seguridad de las organizaciones. Esta propuesta es particularmente importante porque permite la reflexión sobre la seguridad más allá de los límites físicos en la medida en que brinda elementos técnicos para articular la protección de los datos a la estructura que en este caso responde a la propuesta por la ISO/IEC 27001.

Ahora, respecto de los desafíos que presenta la protección de datos circulantes en internet, Galvis [36] en su documento “Protección de datos en Colombia, avances y retos” plantea sus aportes hacia la seguridad jurídica y el reconocimiento de los derechos fundamentales como la habeas data, intimidad, honra y buen nombre, información y libertad informática según las exigencias internacionales. Este estudio permite identificar los principios sobre los que se debe orientar la protección de datos y que servirá de base para la articulación entre la Ley Estatutaria 1581 de 2012 y la Norma ISO 27001, los cuales son: diseño de las políticas internas de privacidad de la compañía, la toma de decisión simplificada para los usuarios a la hora de entregar sus datos y una mayor transparencia a la hora de recolectar los datos. El documento concluye que con el fin de que la Ley 1581 de 2012 se pueda implementar para facilitar el complimiento es necesario reglamentar aspectos relacionados con la autorización del Titular para que se pueda llevar a cabo el tratamiento de sus datos personales, deben establecerse las políticas de tratamiento de los responsables y encargados, los derechos de los Titulares de información, las transferencias de datos personales, las normas corporativas vinculantes y la responsabilidad demostrada, entre otros aspectos. De la misma manera, es importante definir los lineamientos y

términos para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones.

Más recientemente, Pelloso, Aparecido, Frogeri y Leal [37] en el documento titulado “A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos” se propusieron describir la dinámica de las organizaciones brasileras en cuando a la adecuación de las Ley General de Protección de Datos Personales promovida por el Estado brasilero para la manipulación, tratamiento y almacenamiento de datos personales por las organizaciones. El abordaje metodológico es descriptivo de tipo transversal con enfoque cualitativo por medio de un estudio de casos múltiples. Los datos fueron obtenidos a partir entrevistas semiestructuradas con siete profesionales encargados de la recolección y almacenamiento de los datos de la empresa. El estudio encontró que las empresas no están preparadas para responder con las regulaciones establecidas, requiriéndose considerables cambios técnicos y de gestión en las áreas de tecnología de información e seguridad de la información.

2.1.3 Automatización del Sistema de Gestión para La Seguridad De La Información

Dentro de los estudios que han abordado el tema de la automatización de un sistema de seguridad de la información se encuentran los siguientes:

Curtis [39] en su documento titulado “Integrated Control and Safety” se propone identificar los beneficios de integrar el control y la seguridad a partir de la adopción de nuevas técnicas y tecnologías, las cuales representan ventajas a nivel de los costos y específicamente en la seguridad de la información, no obstante, los autores sugieren considerar su pertinencia antes de adoptarlos, además de aconsejar

sistemas de seguridad diseñados desde el principio para poder contemplar la causa común, la seguridad y la ciberseguridad. Consejo que justamente guía la propuesta, ya que el sistema de seguridad basado en la Norma ISO/IEC 27001 se diseñará e implementará desde el principio logrando la articulación con la Ley que regula la protección de datos personales en Colombia.

Montesino, Baluja, Porvén [23], “Gestión automatizada e integrada de controles de seguridad informática” proponen un modelo integrador para la automatización de la seguridad de la información basado en sistemas de gestión de información y eventos de seguridad (SIEM) para optimizar la efectividad de los controles implementados y disminuir la gestión de la seguridad de la información. Sobre la consideración de que automatizar implica la operación, monitoreo y la revisión de los controles de manera automática mediante hardware y software y sin la intervención humana, los autores priorizaron los controles que requerían ser automatizados a fin de lograr el objetivo de la seguridad de la información. Para el caso, los controles que se automatizarán corresponden a los que surjan a partir de la articulación entre la Norma ISO/IEC 27001, la Ley 1581 de 2012 y las necesidades particulares del contexto de estudio. Esto implica que se debe realizar un proceso profundo de personalización y adaptación del sistema SIEM utilizado para aplicar el modelo propuesto, mediante la definición de conectores, políticas, reglas de correlación y reportes de seguridad informática.

Venegas y Pardo [40] en su documento titulado “Hacia un modelo para la gestión de riesgos de TI en MiPyMEs : MOGRIT” presentan las bases sobre las cuales se articulan los modelos de riesgos de las Tecnologías de la Información como CRAMM, COBIT, EBIOS, ITIL V3 MAGERIT, OCTAVE, con algunas Normas enfocadas a prevenir los riesgos como las Normas de la familia ISO/IEC 27000. El estudio tuvo un

enfoque comparativo que permitió evidenciar la mayoría de las Normas y modelos están relacionadas entre sí, pese a que algunas de ellas presentan procesos más detallados, con un nivel más profundo entre ellas.

En la misma línea de los estudios sobre la automatización de procesos, Martelo, Madera y Betín [41] en su investigación titulada “Software para la Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI)”, se propusieron el desarrollo de un software para controlar los documentos generados tras la implantación del SGSI. Para soportar dicho software, se diseña e implementa un modelo que define acciones de gestión necesarias para la aprobación, revisión, actualización, estados y legibilidad en documentos durante el ciclo de vida del SGSI. Como resultado, la herramienta dentro de sus funciones trabaja dentro de manera cíclica en los procesos estandarizados de la Norma ISO/IEC 27001 para reconocer el estado de los documentos; gestión de la información para evitar la utilización de documentos que ya expiraron; la gestión de funciones y actividades; garantiza acceso, accesibilidad y seguimiento a documentos asignados. Esta función es particularmente importante para garantizar un buen desarrollo de la seguridad de la información, por lo cual, la identificación de la herramienta que permitirá la automatización del SGSI en la institución deberá garantizar dichas funciones.

Recientemente, Syreyshchikova, Pimenov, Mikolajczyk, Moldovan [42] en su estudio titulado “Information Safety Process Development According to ISO 27001 for an Industrial Enterprise” plantean como objetivo proteger la información de base industrial de acuerdo con la norma ISO 27001. Para su cumplimiento emplean varias herramientas basadas en software para responder con los requisitos de dicha Norma. Dentro de los resultados se garantizó la disponibilidad de datos para usuarios

autorizados; la capacidad de obtener rápidamente servicios de información; la integridad de la información según su relevancia y seguridad contra alteraciones no autorizadas o destrucción y la confidencialidad de la información de la empresa. En conjunto, la implementación del software de “registro y auditoría” permite, de acuerdo con los autores, la creación de un plan de continuidad para minimizar los riesgos y maximizar el retorno de la inversión, las oportunidades del negocio y el cumplimiento.

Narain y Gupta [43] “Information Security Management Practices: Case Studies from India” se proponen explorar y examinar las prácticas de la seguridad de la información en dos organizaciones de desarrollo y servicios de tecnología de la información en la india.

En el diseño del estudio de casos, el estudio adopta la vía de la investigación cualitativa para comprender las prácticas actuales de GSI de las organizaciones del caso. Las observaciones derivadas de las entrevistas semiestructuradas se presentan mediante una metodología de análisis descriptivo. Además, se utiliza el método de indagación SAP-LAP (Situación, Actor, Proceso-Aprendizaje, Acción, Desempeño) para analizar los resultados de la investigación. Los resultados muestran el apoyo alineado por parte de la alta gerencia, la construcción de una cultura de seguridad de la información dentro de la organización y un sistema de vigilancia para el desarrollo eficaz del sistema de gestión de la información son aspectos que resultan importantes para el desarrollo posterior a la implantación de SGSI, ya que al ser un esquema nuevo de organización generará cambios y procesos de adaptación por parte de los agentes de la organización, especialmente los colaboradores del Departamento de Sistemas.

Finalmente, Varela, Parody, Gasca y Gómez [44] en su investigación titulada “Automatic Verification and Diagnosis of Security” proponen un método de evaluación

de riesgos para el análisis de la seguridad dentro de un proceso comercial que no se encuentra a conformidad con un nivel de riesgo aceptable. Para lograr este objetivo, los autores utilizaron una extensión del proceso de negocios con información de riesgo de seguridad y realizaron el siguiente proceso: 1) implementaron un algoritmo para verificar el nivel de riesgo de modelos de procesos; 2) diseñaron un algoritmo para diagnosticar el riesgo de las actividades que no se ajustan al nivel de riesgo establecido en los objetivos de seguridad-riesgo; y 3) aplicaron un instrumento que apoyó la propuesta. Además, se presentó un estudio de caso real, un conjunto de puntos de referencia de escalabilidad de rendimiento y se lleva a cabo un análisis para comprobar la utilidad e idoneidad de la automatización de los algoritmos. Según los autores es el primer trabajo que aborda la conciencia del riesgo de procesos comerciales de manera automatizada y resulta particularmente importante para los alcances posteriores a este estudio.

En conclusión, el recorrido de los antecedentes de la investigación sobre la Norma ISO/IEC 27001, la protección de los datos personales y la automatización de sistemas de seguridad de información ofrecen elementos importantes a considerar durante la propuesta metodológica y el desarrollo de la investigación; otros por su parte se plantean como sugerencias para las mejoras que requerirá el sistema de gestión de la seguridad de la información cuando se esté ejecutando para responder a las necesidades de la institución universitaria.

2.1.4 Eramba como herramienta de automatización

La elección del software Eramba como herramienta para automatizar tuvo su razón, en primera instancia, en las características de acceso abierto que proporciona y la posibilidad de articular los requisitos de la norma ISO 27001 con las exigencias de la Ley 1581. No obstante, resultaron sugerentes los aportes provenientes de la

literatura donde en investigaciones empíricas emplearon Eramba para adelantar tareas similares, mencionando así: 1. que el software facilita la interoperabilidad semántica y permite priorizar las actividades durante la supervisión del cumplimiento para las empresas. Así mismo, 2. permite la adaptación de una solución en la nube y 3. el ingreso de nuevos controles de seguridad a partir de la base que proporciona la herramienta, lo que facilita la adaptación al contexto de la información y a las necesidades de la empresa.

Con respecto al primer punto a favor de la utilización de la herramienta, Cheng y Lim-Cheng [72] ubican su análisis en la complejidad que trae consigo la globalización para los procesos de gobernanza, gestión de riesgos y cumplimiento, que exigen un acercamiento a múltiples normas para responder con las regulaciones existentes según sea el caso, frente a lo que se busca la optimización de procesos reduciendo la redundancia en el trabajo de las organizaciones, objetivo que según el estudio se logró con Eramba dada en la facilidad de la interoperabilidad semántica.

El estudio de Duarte [73] respalda el uso de Eramba para las pequeñas y medianas empresas dada la poca disponibilidad e recursos económicos, en las cuales se acostumbran herramientas de código abierto, entre las que se encuentra Eramba, porque a diferencia de otras esta permite que se sorteen problemas de soporte, migración de datos, escalabilidad y las actualizaciones con el almacenamiento en la nube a largo plazo

En esta misma línea del almacenamiento en la nube que proporciona Eramba, Tenorio [74] rescata las ventajas al respecto en tanto facilita la consulta de administradores, mantiene las vulnerabilidades actualizadas para determinar las brechas de seguridad.

2.2 Bases Teóricas

Los antecedentes expuestos, así como el marco legal que soporta la protección de datos personales, dan cuenta de la necesidad real que tienen las organizaciones frente al riesgo informático, pues cada vez son más sofisticados los ataques piratas a las infraestructuras de organizaciones privadas y de instituciones públicas, los cuales tienen variadas motivaciones: desde la mera especulación y diversión por parte de piratas informáticas que se complacen con desnudar las vulnerabilidades informáticas, hasta quienes se dedican al comercio ilegal de la información hurtada.

El diseño y automatización del SGSI basado en la ISO/IEC 27001:2013 da cumplimiento de manera ágil a la Ley 1581 de 2012 de protección de datos personales y a su vez permite que el Departamento de Sistemas de una institución universitaria en Colombia optimice y haga seguimiento a sus procesos de una manera ágil.

A continuación, se presentan los principales planteamientos teóricos sobre la seguridad de la información, el SGSI basado en la ISO 27001 y los conceptos que de allí se desprenden.

2.2.1 Sistema De Gestión De La Seguridad De La Información Basado En La Norma ISO 27001

Según esta Norma ISO 27001, un Sistema de Gestión de la Seguridad de la Información es una parte del Sistema de Gestión General de las organizaciones, el cual está basado en un enfoque de riesgo, el cual se crea para: implementar, operar, supervisar, mantener y mejorar la seguridad de la información que se administra en una organización privada o en una institución pública.

Con el diseño e implementación de un SGSI que cumpla con los lineamientos de la ISO 27001, las organizaciones pueden obtener beneficios como:

- Analizar los riesgos, vulnerabilidades y amenazas que desafían la gestión en la organización.
- Conocer a profundidad el funcionamiento de la organización y actuar eficazmente ante los riesgos que se le presentan en su seguridad informática.
- Cumplir con los acuerdos y Normas internacionales; además de la Normatividad nacional en lo relacionado con la seguridad de la información, especialmente a la protección de datos personales, comercio electrónico y propiedad intelectual [9].

2.2.2 Proceso de Diseño de un SGSI

Para la ISO un Sistema de Gestión es un proceso que se define a partir de cuatro etapas: planificar, Implementar, Medir y Mejorar [48]. Esta metodología se puede aplicar a todos los procesos del SGSI para procurar una mejora continua en la gestión de la información en las organizaciones privadas y en las instituciones públicas.

De acuerdo al autor Baldecchi [48], las fases del modelo incluyen las actividades que reporta la Tabla 1:

Tabla 1. *PIMM (Planear, Implementar, Medir y Mejorar)*

Etapa	Descripción
Planificar (Establecer el SGSI)	Establecer la política, objetivos, procesos y procedimientos del SGSI pertinentes a la administración del riesgo y optimizar la seguridad de la información para lograr los resultados de conformidad con las políticas y objetivos de la organización.

Implementar **(Implementar y operar el SGSI)**	Poner en funcionamiento y llevar a cabo la política, los controles, los procesos y los procedimientos del SGSI.
Medir **(Monitorear y revisar el SGSI)**	Monitorear, y hasta donde se pueda aplicar, evaluar el rendimiento del proceso contra la política del SGSI, sus objetivos y experiencia práctica, e informar los resultados para gestionar su revisión
Mejorar **(Mantener y mejorar el SGSI)**	Tomar acciones correctivas y preventivas basadas en los resultados de auditorías internas del SGSI y de revisión de gestión u otra información relevante, para lograr la mejora continua del SGSI.

Nota. Tomado de Implementación efectiva de un SGSI ISO 27001

2.2.3 Requerimientos que exige la Norma ISO 27001:2013

En la consideración de que la Norma ISO 27001 brinda un enfoque integrado de la seguridad de la información y para su diseño e implementación es necesario cumplir con los requerimientos que se listan en la Tabla 10, que permitan comprender el contexto de la organización, aspectos de liderazgo y compromiso con los requisitos del SGSI, planificación, soporte, operación, evaluación de desempeño y mejora.

Tabla 2. *Requisitos de la Norma ISO 27001:2013*

Sección	Requerimientos ISO 27001
4	Contexto de la organización
4.1	Comprensión de la organización y de su contexto
4.1	Determinar los objetivos del SGSI de la organización y cualquier problema que pueda afectar su eficacia
4.2	Comprensión de las necesidades y expectativas de las partes interesadas
4.2 (a)	Identificar las partes interesadas incluyendo leyes aplicables, regulaciones, contratos, etc.

4.2 (b)	Determinar los requerimientos y obligaciones relevantes de seguridad de la información
4.3	Determinación del alcance del SGSI
4.3	Determinar y documentar el alcance del SGSI
4.4	SGSI
4.4	Establecer, implementar, mantener y mejorar de forma continua el SGSI acorde al estándar
5	Liderazgo
5.1	Liderazgo y compromiso
5.1	La administración debe demostrar liderazgo y compromiso por el SGSI
5.2	Política
5.2	Documentar la Política de Seguridad de la Información
5.3	Roles, responsabilidades y autoridades en la organización
5.3	Asignar y comunicar los roles y responsabilidades de seguridad de la información
6	Planificación
6.1	Acciones para tratar los riesgos y oportunidades
6.1.1	Diseñar el SGSI para satisfacer los requerimientos, tratando riesgos e identificando oportunidades
6.1.2	Definir e implementar un proceso de análisis de riesgos de seguridad de la información
6.1.3	Documentar e implementar un proceso de tratamiento de riesgos de seguridad de la información
6,2	Objetivos de seguridad de la información y planificación para su consecución
6,2	Establecer y documentar los planes y objetivos de la seguridad de la información
7	Soporte
7.1	Recursos
7.1	Determinar y asignar los recursos necesarios para el SGSI
7.2	Competencia
7.2	Determinar, documentar hacer disponibles las competencias necesarias
7.3	Concienciación
7.3	Implementar un programa de concienciación de seguridad
7.4	Comunicación
7.4	Determinar las necesidades de comunicación internas y externas relacionadas al SGSI
7.5	Información documentada

7.5.1	Proveer documentación requerida por el estándar más la requerida por la organización
7.5.2	Proveer un título, autor, formato consistente, revisión y aprobación a los documentos
7.5.3	Mantener un control adecuado de la documentación
8	Operación
8.1	Planificación y control operacional
8.1	Planificar, implementar, controlar y documentar el proceso de gestión de riesgos del SGSI (Tratamiento de riesgos)
8.2	Apreciación de los riesgos de seguridad de la información
8.2	Evaluar y documentar los riesgos de seguridad regularmente y cuando hay cambios
8.3	Tratamiento de los riesgos de seguridad de la información
8.3	Implementar un plan de tratamiento de riesgos y documentar los resultados
9	Evaluación del desempeño
9.1	Seguimiento, medición, análisis y evaluación
9.1	Realizar un seguimiento, medición, análisis y evaluación del SGSI y los controles
9.2	Auditoría interna
9.2	Planificar y realizar una auditoría interna del SGSI
9.3	Revisión por la dirección
9.3	La administración realiza una revisión periódica del SGSI
10	Mejora
10.1	No conformidad y acciones correctivas
10.1	Identificar, arreglar y reaccionar ante no conformidades para evitar su recurrencia documentando todas las acciones
10.2	Mejora continua
10.2	Mejora continua del SGSI

Nota. Elaborada a partir de los requerimientos de Norma ISO 27001:2013

2.2.4 Requerimientos que exige la Ley 1581

Los requerimientos que exige la Ley 1581 de 2012 para la Protección de Datos Personales fueron publicados por la Superintendencia de Industria y Comercio -SIC- (2016) a través de dos listados de comprobación: el primero hace referencia a los 86 principios y deberes establecidos (ver Anexo 1).

Con respecto al primer listado de principios y deberes, la estructura se organiza en quince ítems que se señalan a continuación y se desglosan en el Anexo 1:

- Principios para el tratamiento de datos personales
- Tratamiento De Datos Sensibles y de Menores de Edad
- Derechos de los titulares de información
- Autorización para el tratamiento de datos personales
- Información mínima a los titulares
- Suministro de la información personal
- Atención de consultas y reclamos de los titulares
- Atención de consultas y reclamos de los titulares
- Política de tratamiento de datos personales
- Aviso de privacidad
- Reporte de violaciones a los códigos de seguridad
- Gestión de encargados del tratamiento
- Transferencia y transmisión internacional de datos personales
- Responsabilidad demostrada
- Registro nacional de bases de datos

2.2.5 Automatización de un SGSI

Históricamente, la automatización aparece con la industrialización de los procesos de producción. Es en ese momento donde surgen las máquinas para que alcanzar una producción a gran escala, lo que generó transformaciones en la forma de trabajar, de impactar el mercado y la economía. Esta fue la primera base para que se avanzara hacia la automatización, la cual en la actualidad ya no es una

herramienta de trabajo deseable sino necesaria para mejorar procesos y competir en el mundo globalizado [51]. Por tanto, el interés es contribuir a la reducción del tiempo que dedica un colaborador en el desarrollo de una actividad específica para que su conocimiento sea puesto al servicio del mejoramiento de los mismos procesos.

En este sentido y pensando la automatización para fines de la seguridad de la información, Montesino, Fenz y Baluja [52], ofrecen la definición estándar de automatización como la técnica o método para operar y controlar procesos mediante dispositivos electrónicos, reduciendo al mínimo la intervención humana, lo que no quiere decir que se prescinda de ella. En términos de seguridad de la información, la automatización es requerida para tres objetivos la conservación de la confidencialidad, integridad y disponibilidad de la información, los cuales requieren de controles que deben establecerse, aplicarse, operarse, vigilarse, evaluarse y mejorarse para garantizar el cumplimiento de dichos fines [52].

En los términos que lo enuncian los autores siguiendo los objetivos de la automatización, se dio propuesta planteada en esta investigación respecto SGSI de la Universidad, ya que permite una administración de manera centralizada. Esta claridad respecto del alcance de automatización indica que no es lo mismo automatizar la seguridad de la información que gestionarla. Dos dimensiones que llevan a la necesaria distinción entre seguridad informática e información de la información.

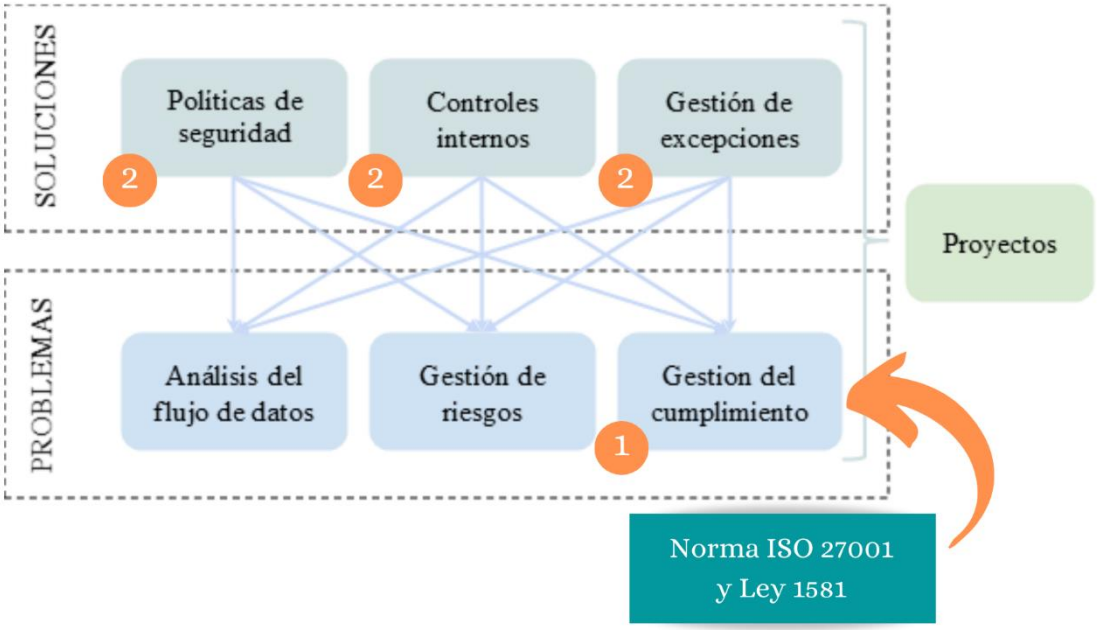
Al respecto, Romero, Figueroa, Vera, Álava, Parrales, Álava, Murillo y Castillo [10] mencionó que es común la confusión entre ambos conceptos, que de parecer similares recaban diferencias sustanciales, ya que mientras la seguridad informática atiende a los medios informáticos que permiten los procesos, técnicas y métodos para procesar, almacenar y transmitir la información, la seguridad de la información no solo

se ocupa de aquellos, sino de todo lo que gestiona información en una organización que es básicamente todo. De acuerdo con ello, puede afirmarse entonces que la seguridad de la información conserva un carácter más completo que la seguridad informática.

Se aclara, de acuerdo con dicha distinción, que, si bien esta investigación se ocupa de la seguridad de la información, la intención de la investigación no es automatizar la seguridad de la información, ya que se requeriría de esfuerzos y recursos mayores que involucran al actor institucional y su planeación, tampoco se está atendiendo a la seguridad informática ya que directamente la intención no es ocuparse los medios por los que discurre la información. Lo que se busca es automatizar el SGSI a partir de las directrices que proporciona la norma ISO 27001 para responder a los lineamientos de la Ley 1581 que en Colombia regula la protección de los datos personales.

En este sentido, para la automatización se propone el programa Eramba Community ya que permite una interrelación entre sus componentes. Al articularlo con la Norma ISO 27001 y la Ley 1581 permite un resultado inicial según se observa en la Figura 3. El diseño que propone Eramba Community identifica los problemas en primera instancia, para luego ofrecer las soluciones y establecer la relación entre ellos. Su operación se facilita mediante el uso de notificaciones, filtros e informes.

Figura 1. Visualización del marco lógico de la herramienta Eramba Community en relación con la Norma ISO 27001 y Ley 1581



Ahora bien, el hecho de que el diseño se estructure mediante problemas y soluciones no indica que Eramba Community los incluye, el programa no viene con bases de datos precargadas con controles, políticas o excepciones, por lo tanto, es necesario identificarlos y documentarlos. Esto puede ser un reto a nivel de proceso ya que si no se hace correctamente podría dificultarse la configuración. Lo único que incluye son los requisitos de cumplimiento, los cuales son los que permiten gestionar el contenido de cumplimiento, que para el caso responden a la Norma ISO 27001 y la Ley 1581.

Entonces, el proceso se inicia con la gestión del cumplimiento y respectivamente se aplican los componentes de solución que se observan en la Figura 3. Para el análisis de riesgo o de flujo de datos los pasos son los mismos y se ejecutan una vez se ha llevado a cabo la gestión del cumplimiento.

2.2.6 Metodología para análisis de riesgos

Para el análisis de riesgos -AR- se tuvo en cuenta la aplicación que ofrece de manera gratuita el Instituto Nacional de Ciberseguridad INCIBE [54], cuyo desarrollo tiene como soporte Microsoft Excel.

Descripción de la aplicación:

La aplicación en mención ha sido diseñada como una herramienta para simplificar el análisis de riesgos. Cada una de las hojas contiene lo siguiente:

- «Ejemplo de análisis»: es un ejemplo de análisis de riesgos que se puede usar como una recomendación para hacer la tares.
- «Tablas AR»: contiene tablas que orientan la manera de hacer las evaluaciones de la probabilidad y el impacto de acuerdo a un rango de tres valores.
- «Catálogo amenazas»: muestra las principales amenazas a analizar en el dominio de una verificación de peligros de seguridad.
- «Activos»: es un listado con los activos establecidos para cada tipo de organización planteado en las disposiciones al concluir la tarea.
- «Cruces Activo-Amenaza»: usado para definir las amenazas que impactan a los activos del modelo escogido.
- «Análisis de Riesgos»: usado para hacer la evaluación de los riesgos Es importante mostrar la probabilidad y el impacto de los riesgos que afectan a cada uno de los activos.

Funcionamiento de la aplicación:

- Lo primero: en «Activos» hay una columna con el nombre «aplicación». Esa columna tiene un listado con dos opciones (SI/NO). Se debe diligencia con «SI» los activos que se usen de acuerdo al tipo de organización que se haya escogido (lo demás se puede dejar en blanco o diligenciar con «NO»).

- Segundo: en «Cruces Activo-Amenaza» se detallan en la primera columna todas las amenazas y en la primera fila los índices de activos (que se relaciona con los de «Activos»). El propósito de es incorporar un «SI» (igual que en lo primero) en la relación entre activo y amenaza para que posterior se presenten de manera automática en «Análisis de Riesgos».

- Tercero: en «Análisis de Riesgos» se selecciona el botón «Mostrar activos» (en la esquina superior izquierda). Ese botón enseñará automáticamente todos los activos seleccionados, con cada una de las amenazas relacionado con esos activos.

- Cuarto: en «Análisis de Riesgos» se escoge la probabilidad y el impacto de cada amenaza relacionado con el activo (es otra lista, con tres opciones Bajo (1), Medio (2), Alto (3)). Cuando se hayan escogido se enseñará en la columna riesgos un número que representa el riesgo de acuerdo con la «Tablas AR» y el fondo de la celda del color respectivo.

Tablas para estimar los riesgos

Las tablas AR serán la guía que permitirán evaluar el riesgo de acuerdo con las escalas de probabilidad e impacto.

La Tabla 5 se enfoca a estimar la probabilidad en un nivel de importancia de 1 a 3 donde 1 es el grado más bajo y 3 es el grado más alto. La Tabla 6 para estimar el impacto maneja una la misma escala de valor de la primera y por último se presenta la Tabla 7 con la escala de aceptación del riesgo con un rango inferior y superior a 4, donde el primero señala una perspectiva de riesgo bajo y el segundo considera un riesgo que debe ser mitigado. De manera integrada, la Figura 2 presenta la convergencia de las tres tablas, por medio de la cual se procede a realizar la estimación de riesgo.

Tabla 3. *Tabla para considerar la probabilidad.*

Valor	Explicación
Bajo (1)	El riesgo se lleva a cabo por lo menos una vez cada año.
Medio (2)	El riesgo se lleva a cabo por lo menos una vez cada mes.
Alto (3)	El riesgo se lleva a cabo por lo menos cada semana.

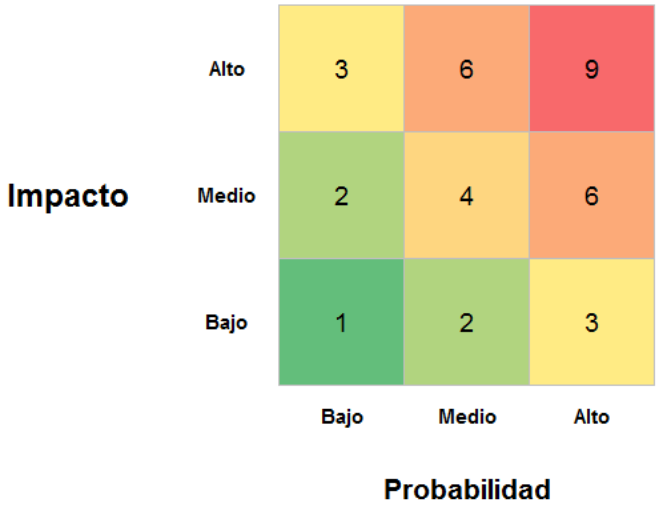
Tabla 4. *Tabla para considerar el impacto*

Valor	Explicación
Bajo (1)	El daño ocasionado por efecto del impacto no tiene resultados importantes para la organización.
Medio (2)	El daño ocasionado por efecto del impacto no tiene resultados críticos para la organización.
Alto (3)	El daño ocasionado por efecto del impacto no tiene resultados graves para la organización.

Tabla 5. *Criterios de aprobación del riesgo*

Rango	Explicación
Riesgo <= 4	La organización contempla el riesgo poco crítico.
Riesgo > 4	La organización considera el riesgo crítico y debe ejecutar su tratamiento.

Figura 2. *Tabla relacional de riesgo, impacto y probabilidad*



Nota. Tomado del Instituto Nacional de Ciberseguridad [54].

El listado de amenazas

El listado de amenazas fue tomado de un extracto modificado del catálogo de amenazas de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información -Magerit- promovida por el Consejo Superior de Administración Electrónica -CSAE- [10]. De esta manera, el siguiente es el catálogo usado para el análisis de riesgos que se hace al DSI y más adelante en la Tabla 8 se presenta el listado de activos del DSI, con los cuales se realiza el análisis amenaza-activo.

Tabla 6. *Catálogo de amenazas MAGERIT*

Amenaza/Activo
Fuego
Daños por agua
Desastres naturales
Fuga de información
Introducción de falsa información
Alteración de la información
Corrupción de la información
Destrucción de información
Interceptación de información (Interceptación auditiva o digital)
Corte del suministro eléctrico
Condiciones inadecuadas de temperatura o humedad
Fallo de servicios de comunicaciones
Interrupción de otros servicios y suministros esenciales
Desastres industriales
Degradación de los soportes de almacenamiento de la información
Difusión de software dañino
Errores de mantenimiento / actualización de programas (software)
Errores de mantenimiento / actualización de equipos (hardware)

Caída del sistema por sobrecarga
Pérdida de equipos
Indisponibilidad del personal
Abuso de privilegios de acceso
Acceso no autorizado
Errores de los usuarios
Errores del administrador
Errores de configuración
Denegación de servicio
Robo
Extorsión
Ingeniería social

Nota. Tomado de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información -Magerit- versión 3.0.

Para este análisis de riesgos en el DSI se han definido los siguientes activos (ver Tabla 9)

Tabla 7. *Activos del Departamento de Sistema*

Identificador	**Activo**
C1	Computadores y servidores (web, BD, archivos, dominio, DNS)
C2	Conexión a Internet cableada
C3	Conexión a Internet con wifi
C4	Celulares con datos y apps para su trabajo
C5	Sitio web y redes sociales que gestionan desde la empresa
C6	Herramientas para empresas en la nube (G Suite, Office 365)

C7	Firewall y Switches
C8	Software
C9	Impresoras

2.3 Marco conceptual

2.3.1 Automatización

En este sentido, Ruedas [51] define la automatización industrial como el uso de sistemas computarizados para controlar las funciones de las máquinas y los procesos para los cuales se usan, llevando así a la sustitución de la operación humana. Sin embargo, aquí hay que hacer hincapié en una diferenciación clave respecto de la automatización en un contexto de fábrica, donde se requiere mano de obra para la producción como por ejemplo las empaquetadoras, clasificadoras o las ensambladoras, lo que implica una reducción de mano de obra; ya que por otro lado está la automatización para la mejora de procesos administrativos o de recurso humano, donde se requiere ya no la mano de obra sino el conocimiento.

En este sentido, las soluciones de automatización, de acuerdo con Mitsubishi Electric [56], deben privilegiar la economía, fiabilidad y flexibilidad con el objetivo de satisfacer las demandas de entornos cada vez más cambiantes para responder a las exigencias del mercado. De ahí que las inversiones en esta materia sean un factor

clave para fortalecer e incrementar el rendimiento hacia la obtención de beneficios claramente definidos.

2.3.2 La Norma ISO 27001:2013

La Norma ISO 27001 permite un enfoque integrado de la seguridad de la información, eso requiere que la evaluación del riesgo se haga sobre todos los activos de la organización, incluyendo hardware, software, documentación, personas, proveedores, socios entre otros, y elegir los controles aplicables para disminuir esos riesgos.

Generalmente se ve en la Norma ISO 27001 una sobrecarga para la gestión de TI por la cantidad de documentos que se deben crear e implementar, pero realmente es una herramienta que permite mejorar los procesos, organizar lo que se tiene en TI y disminuir los riesgos de la información y en particular de los datos personales [17].

2.3.3 Cumplimiento de la Ley 1581 de 2012

Colombia cuenta con un marco legal para la protección de datos personales desde la Constitución de 1991 en su Artículo 15, en el cual se establece que:

> Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

Debido a que el derecho a la privacidad está consagrado en el capítulo I de la Constitución se reconoce que es de aplicación inmediata por hacer parte de los derechos fundamentales, sin embargo, solo fue hasta el 16 de diciembre de 2010 que

el Congreso de Colombia aprobó el Proyecto de Ley Estatutaria No 184 de 2010 Senado y 046 de 2010 Cámara que contiene “disposiciones generales para la protección de datos personales”, la cual, para su entrada en vigor requería una revisión por parte de la Corte Constitucional así como una resolución por escrito de la Corte y la ratificación del presidente que ocurrió hasta el 6 de octubre de 2011 [16].

Dicho preámbulo, sienta las bases para la Ley 1581 de 2012 que constituye el marco general de la protección de los datos personales en Colombia, la cual desarrolla el derecho constitucional que tienen todas las personas a:

> […] conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Dicha Ley Estatutaria sanciona específicamente la violación de datos personales cuando una persona/entidad, sin autorización y en beneficio propio o de un tercero, obtiene, compila, sustrae, ofrece, vende, intercambia, envía, compra, intercepta, difunde, modifica o utiliza datos personales contenidos en ficheros, archivos, bases de datos o medios similares con pena de prisión de 48 a 96 meses y con multa 100 a 1000 salarios mínimos legales mensuales vigentes.

De esta manera, en el ámbito estatutario, la Ley 1581 de protección de datos hace operativo el derecho constitucional de todos los individuos a conocer, actualizar y corregir datos personales en bases de datos o archivos, sean estos públicos o privados. Además, en su revisión de la Ley, la Corte Constitucional estableció que la constitucionalidad de Ley 1581 de protección de datos establece que los individuos tienen derecho a borrar esa información, creando así cierto paralelismo con los

derechos a acceder, rectificar, cancelar y oponerse (ARCO) al procesamiento de datos personales [13].

Ahora, tras la aprobación de la Ley 1581 en 2012, existen esfuerzos anteriores que señalan el camino hacia la aprobación de dicha Ley. En este sentido, el Congreso de la República modificó el Código Penal mediante la Ley 1273 de 5 de enero de 2009 con lo cual se crea un nuevo bien jurídico tutelado, denominado “protección de la información y de los datos”. De esta forma se establecen nuevos delitos penales relacionados con el uso de computadoras, la protección de la información y la protección de datos personales con penas de cárcel hasta de 120 meses y multas de hasta 1500 veces el salario mínimo legal vigente [16].

Otro antecedente indica que la Ley 1266 promulgada en 2008 establece también las disposiciones generales del habeas data y regula el manejo de la información contenida en bases de datos personales, en particular las de carácter financiero, crediticio, mercantil y de información, así como la información de terceros países [11].

El concepto “Habeas data”, en el ámbito constitucional es un recurso conocido que:

> […] establece que los individuos tienen derecho a su intimidad personal y familiar y a su buen nombre. El Estado debe respetar este derecho y garantizar que sea respetado por otros. El individuo tiene de igual modo derecho a conocer, actualizar y rectificar los datos que se hayan recogido sobre él en bancos de datos y en archivos públicos y privados [10].

A su vez, la Ley 79 de 1993, regula el levantamiento del censo a nivel nacional y establece los procedimientos para procesar los datos personales en ese contexto [16].

De esta manera, las leyes 1266, 1273 y la 1581 de 2012 (Ley de Protección de Datos Personales) aplican a entidades tanto públicas como privadas, mientras que la Ley 79 se aplica exclusivamente a la entidad encargada de realizar los censos públicos.

En cuanto a los mecanismos de ejecución para poner en práctica los ordenamientos de las leyes sobre protección de datos, el principal de ellos se encuentra en la Ley 2591 de 1991 y en las disposiciones relacionadas con la protección de datos mencionadas anteriormente. Tanto la Ley 1266 de 2008 como la Ley 1581 de protección de datos establecen por vía administrativa el procedimiento de consulta que procede ante el responsable o encargado del tratamiento o el de reclamo que procede directamente ante la autoridad de control. Para ejercer este último, debe haberse primero surtido el proceso de consulta en caso de que el titular considere que se está dando algún tipo de vulneración en el tratamiento de su información.

La Ley 1581 de protección de datos dispone que la persona puede consultar y conocer su información personal en cualquier base de datos pública o privada. La consulta será hecha utilizando el procedimiento dispuesto por el procesador de los datos y será atendida en un plazo máximo de 10 días hábiles a partir de la fecha de recepción. Cuando no sea posible atender la solicitud de consulta en el plazo indicado, el procesador informará a la persona las razones del retraso y la fecha en que se le atenderá. En cualquier caso, el retraso no excederá cinco días hábiles después del vencimiento del primer plazo [16].

En general puede decirse, que la protección de datos personales presenta un amplio marco constitucional y legal que obliga a las instituciones públicas y privadas

a proteger la información que tienen de los ciudadanos en las diversas bases de datos. De no cumplir con los requerimientos exigidos por el marco legal y Normativo, las organizaciones pueden enfrentar procesos administrativos que pueden tener consecuencias penales para los responsables, además de elevadas multas económicas.

Protección de datos/autoridades ejecutoras.

En Colombia existen dos autoridades administrativas encargadas de la ejecución de las leyes y Normas sobre privacidad/protección de datos:

- La Superintendencia de Industria y Comercio.
- La Superintendencia Financiera.

La Superintendencia de Industria y Comercio

Es un organismo de carácter técnico, adscrito a la Rama Ejecutiva del Poder Público –Ministerio de Comercio, Industria y Turismo–, entre cuyas funciones se incluye la de velar por el cumplimiento de las Normas sobre protección del consumidor, protección de datos personales, cumplimiento con las Normas de competencia/antimonopolio, gestión del sistema nacional de propiedad industrial, así como asuntos jurisdiccionales en materia de protección al consumidor y competencia desleal. Dentro de la Superintendencia, la Delegatura para la Protección de Datos Personales vela por el cumplimiento de las leyes referentes al procesamiento de datos personales [12].

Cabe mencionar que esta entidad tiene la facultad para impartir instrucciones, realizar auditorías externas o llevar a cabo investigaciones oficiales por iniciativa propia.

Por su parte, la Superintendencia Financiera,

> Es un organismo de carácter técnico, adscrito a la Rama Ejecutiva del Poder Público –Ministerio de Hacienda y Crédito Público– encargada de supervisar el funcionamiento de los mercados financiero y bursátil de Colombia, preservar su estabilidad, seguridad y confianza, así como promover, organizar y desarrollar el mercado de valores y la protección de los inversionistas, ahorradores y asegurados [12].

Para estas dos entidades, los retos aparecen el nivel del riesgo y la variedad de amenazas presentes en los sistemas de información a nivel nacional e internacional en el actual mundo digital propio de la globalización, sin embargo, es importante seguir trabajando en la materia para aumentar el nivel de concientización sobre la gestión de la información en los niveles directivos y operativos de las organizaciones privadas y de las instituciones públicas [12].

2.3.4 *Sistema de Información*

De acuerdo con Meguzzato y Renau [57] un sistema de información comprendido en el contexto de una empresa tiene la función de captar la información, que luego será procesada y puesta a disposición de quienes la requieran dentro del contexto organizacional para la planeación, toma de decisiones y control estratégico. No obstante, aunque los autores no lo contemplan, un sistema de información contribuye a la mejora continua de las organizaciones y la información que se gestiona no solo sirve para los procesos internos, sino también externos.

En este sentido, se entiende, siguiendo a Lapiedra, Devece y Guiral [58], que la información discurre por toda la organización tanto de manera formal como informal,

en sentido horizontal y vertical, lo que indica que el sistema de información representa una estructura organizativa que se encarga de la administración de la información en todas las formas en que se genera y gestiona, de manera eficaz y eficiente para que la organización logre sus objetivos de acuerdo con la planeación y las estrategias de manera colectiva e individual atendiendo a los valores y creencias. Por tanto, el sistema de información es más que un sistema informático, dado que este último hace referencia a la compleja red de conexiones entre dispositivos de hardware y el software.

2.3.5 Seguridad de la Información

La seguridad de la información según Godoy [45] “es un conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos”, su función se enfoca en la protección de la información dentro de los sistemas de la información, lo cual implica tres principios básicos: confidencialidad, integridad y disponibilidad de la misma independiente del medio de almacenamiento. En este sentido, la seguridad se relaciona con la ausencia de riesgo, que no es más que todo lo que pueda afectar el funcionamiento de un sistema y sus resultados.

Frente a la definición de seguridad de la información, es muy importante marcar la deferencia con la seguridad informática, ya que esta solo se encarga de la de la protección del medio informático, el cual puede gestionar información, pero no siempre es el único medio, aún están presentes por ejemplo las formas físicas. No obstante, marcar la diferencia entre ambos conceptos no solo hace parte de una necesidad teórica, sino de una necesidad práctica y técnica para el desarrollo de la presente investigación que en aras de cumplir con el objetivo de automatización del

SGSI requiere tener claras las bases de la seguridad de la información de acuerdo con lo que se debe atender en la seguridad informática.

La seguridad de la información basada en la tecnología debe cumplir según las Normas de cada país, con la condición de confidencialidad, es decir, no porque se maneje por medios tecnológicos indica que debe estar disponible al público, por lo cual, las organizaciones deben velar por su protección si se tiene en cuenta que la información ofrece ventajas competitivas a las empresas. De ahí que la información pueda ser clasificada como crítica, valiosa, sensible, de riesgo y seguridad según Godoy [45].

Ahora, para que la seguridad de la información entre en operación y sea efectiva debe tenerse en cuanto los siguientes aspectos:

- Disponibilidad
- Comunicación
- Identificación de problemas
- Análisis de riesgos
- Integridad
- Confidencialidad
- Recuperación de los riesgos

De otra manera, la seguridad de la información involucra la implementación de estrategias que deben considerar de manera prioritaria las políticas, controles de seguridad, tecnologías y procedimientos para la identificación de riesgos que puedan vulnerar a los activos de información y los sistemas donde se almacena y administra [45].

En términos generales, la información en cualquier tipo de organización o institución presenta amenazas internas, externas y naturales, las cuales pueden atentar contra uno o todos los aspectos mencionados poniendo en riesgo el funcionamiento mismo de los negocios y su continuidad; o generando pérdidas importantes de capital a través del pago de sanciones que por acción u omisión pueden imponer las autoridades a las organizaciones que incumplan con la salvaguarda efectiva de la información siguiendo los estándares internacionales y la Normatividad nacional.

2.3.6 Seguridad Informática

Atendiendo a la distinción entre seguridad de la información y seguridad informática señalada en el anterior numeral, esta última se enfoca en los sistemas de información los cuales están compuestos por redes y arquitectura informática complejas que cada vez cobran importancia en las empresas, no obstante, los sistemas de información señalan la pertinencia de llevar todos los esfuerzos necesarios para, al menos, minimizar los riesgos a los que están expuestos por los ataques de los ciberdelincuentes, así como también los riesgos por pérdida o siniestros [46,47].

De acuerdo con Carpentier [47] existen algunos factores que responden a la necesidad de proteger un sistema de información, unos pueden parecer obvios, otros no siempre están adecuadamente identificados y otros no son de común conocimiento “como las obligaciones y responsabilidad legales de los directivos en relación con el uso y el control del sistema de información”.

En conjunto, estos factores llevan al establecimiento de unos requisitos que permitan la protección general completa del sistema de información, a saber: elaboración de Normas y procedimientos, matriz de acciones y responsables y definición de los riesgos. Estos

requisitos a su vez se presentan como elementos clave dentro de los cuatro principios de seguridad que ya se presentaron dentro del concepto de seguridad de la información y que pueden alcanzarse como oportunidades de solución de seguridad, pero que se amplían si se piensa en la seguridad que requiere un sistema informático [47].

- El no repudio, considerado como el quinto principio, se introdujo en la Norma ISO 7498-2 como servicio de seguridad que pudiera ser emitido por un mecanismo como la firma digital, la integridad de los datos o su registro. El elemento de la prueba de no repudio debe permitir la identificación que representa, requiere ser ubicado en el tiempo (marca de tiempo) y presentar el estado del contexto en el que se ha elaborado (certificados). El no repudio se encuentra a su vez descrito en la Norma ISO/IEC 10181-4 sobre las tecnologías de la información para los sistemas abiertos.
- La autenticación es el método que permite establecer la validez de una solicitud formulada para acceder a un sistema. La autenticidad es la combinación de una autenticación y de la integridad.
- Los mecanismos de cifrado se basan en el principio de que el emisor y el receptor acuerdan una contraseña solo conocida por los dos. El emisor utiliza esta contraseña como clave de cifrado para el mensaje que se ha de transmitir, solo el receptor que conoce esta contraseña la puede utilizar como clave para descifrar el mensaje y acceder a este.

Además, para cumplir efectivamente con los objetivos de un sistema de información se deberá tener en consideración las siguientes condiciones según De Pablo, López, Martín y Medina [46]:

- Confiable: ofreciendo información de calidad y sin errores.
- Selectivo, suministrando solo la información necesaria para el objetivo asignado.
- Relevante, proporcionando información de interés para el usuario.

- Oportuno, entregando la información en el momento necesario.
- Flexible, facilitando su propia modificación para ajustarlo a las necesidades cambiantes de la organización.

2.3.7 Protección de Datos Personales

En Colombia, la Protección de Datos Personales es una Ley que identifica y ampara el derecho de todos los ciudadanos tanto a conocer como rectificar, actualizar e incluso retirarse de las bases de datos en las que se hayan recogido información para manejo por parte de entidades públicas o privadas [4].

En este sentido, es pertinente mencionar que cuando se habla de datos personales se hace referencia a toda información que permita la identificación de una persona, como la identificación, estado civil, fecha y lugar de nacimiento, edad, residencia, profesión, ocupación, así también información catalogada como sensible porque más que una identificación se involucra en la vida íntima de la persona, como la condición de salud, ideología política, condición sexual, lo cual toca el tema de la intimidad. Estos datos que se suministran a diferentes entidades con fines específicos entre las partes, además de distinguirte entre la sociedad, es la que permite la generación de flujos de información con significativas contribuciones al crecimiento económico y mejoramiento de los bienes y servicios.

Para la Superintendencia [4] existen varios tipos de datos personales. Están aquellos de:

- “Dato Público: Es la información que el decreto o la Constitución Política decide de ese modo, así como todos aquellos que no sean semiprivados o privados.

- Dato Semiprivado: Es la información que no tiene característica íntima, discreta, ni pública y cuyo conocimiento o difusión puede importar no sólo a su dueño sino a determinada parte o agrupación de individuos.
- Dato Privado: Es la información que por su condición reservada sólo es importante para el dueño de dicha información.
- Dato Sensible: Es la información que afecta la privacidad del dueño o cuya utilización no debida puede ocasionar su marginación" [4].

Por otro lado, también existen datos personales a los cuales no les atribuye la Ley.

- "A las bases de datos o archivos mantenidos en un dominio únicamente personal o doméstico.
- Las que tengan por objetivo la seguridad y defensa nacional, la prevención, detección, monitoreo y control del lavado de activos y la financiación del terrorismo.
- Las que tengan como objetivo y contengan información de inteligencia y contrainteligencia.
- Las que contengan información periodística y otros temas editoriales
- Las bases de datos con información financiera, crediticia, comercial y de servicios, y de los censos de población y vivienda" [4].

Para Garriga [49] existe un aspecto importante que a su criterio suele quedar implícito dentro del concepto de la protección de datos personales y tiene que ver con el tema de dignidad de la persona en tanto la dignificación y la autonomía, lo que convierte al concepto en una deriva compleja de teorías actualizadas según la historia que, por un lado, muestran la aproximación negativa del derecho frente a no sufrir abusos y por otro lado, el carácter humano frente a valores como la autodisciplina y autodeterminación, en conjunto permiten el desarrollo de la personalidad [50].

Sobre esta línea, Garriga [49] establece la diferencia entre el concepto de protección de datos personales y la intimidad desde al caso español y según la Ley

que los cubre. Para la autora, el derecho de protección de datos dota a una persona de poner sobre el manejo de sus datos, el uso y destino con el fin de impedir un daño hacia la dignidad, lo cual plantea una diferencia con el derecho a la intimidad, ya esta no aporta protección suficiente si se mira de la óptica del progreso tecnológico, lo que convierte en una oportunidad de amenaza a la dignidad y los derechos de la persona por aquello que se denomina como la libertad informática. Por su parte, la protección de datos amplía la garantía constitucional, ya que no solo protege la intimidad de la persona sino cualquier tipo de dato personal que vincule la intimidad o no, cuyo uso por terceras personas pueda afectar su dignidad. Frente a tal distinción de la autora, se ratifica la importancia del concepto de la protección de datos personales como concepto central y general que para efectos de la investigación y de su aplicación en un contexto organizacional, estaría cobijando el tema de la intimidad.

2.3.8 Optimización de procesos

Para Gómez [59], la optimización puede llevarse a cabo tanto para uno como varios objetivos en función de la simultaneidad que se requiera para cumplir con la gestión de los procesos en una organización. En si la optimización está relacionada con la toma de decisiones frente a diferentes alternativas que permitan responder a las situaciones de la mejor manera en cualquier ámbito, o dicho de otro modo es lo que permite que se logre el mejor funcionamiento de algo haciendo el mejor uso de los recursos.

A nivel empresarial la optimización de procesos se refiere según Westreicher [60] a la simplificación de algunos o todos los procedimientos con el fin de que puedan ser adelantados de una manera ágil tanto en reducción de tiempo como en costos.

2.3.9 Optimización del tiempo

La optimización del tiempo es entendida por González [61] como una forma de gestión ya que implica una planificación y distribución del trabajo para que las acciones se lleven a cabo en el momento adecuado. Lo que no quiere decir que tenga que destinarse mayor tiempo para realizar una tarea, sino, justamente lo contrario, hacer un uso adecuado del tiempo disponible. Para lograrlo, Udaondo [62] existen técnicas que permiten alcanzar los objetivos dentro de los tiempos establecidos y resultan adecuadas no solo para la planificación individual sino para la planificación organizacional ya que resulta importante en todas las actividades que implican relacionamiento con los clientes, el horario para desempeñar las actividades y el desarrollo de procesos que tienen tiempos establecidos.

2.3.10 Optimización de Costos

La optimización pensada desde los costos entendida desde la posibilidad de sacar el máximo beneficio con los recursos que dispone una empresa es la forma más adecuada de considerar este tipo de optimización tal como lo sugiere Lozano [63]. Ya que restaría importancia a su función si se entiende como una simple reducción de costos.

En este sentido, el beneficio real se generar al considerar de manera paralela tanto los ingresos como los gastos, razón de ser de las sociedades mercantiles. No se trata, por tanto, de incrementar los primeros o disminuir los segundos para lograr un beneficio, sino de comprender que ambas dimensiones dependen una de la otra

y para el caso, no siempre una disminución de costos generará los beneficios esperados en cuanto a los ingresos.

2.3.11 Mejoramiento Continuo

El mejoramiento o la mejora continua es un término muy utilizado entre la jerga empresarial, en los negocios y hasta la educación; puede decirse básicamente que aplica para cualquier proceso que busca ser mantenido en un nivel de calidad, lo cual implica según Guerra [64], que debe haber un conocimiento de lo que se quiere lograr, para llevar a cabo el monitoreo continuo que permita evaluar el progreso.

Como apoyo a dicho al seguimiento de los procesos están las preguntas correctas, la recolección de datos útiles continua que luego se convierten en la información que permitirá la toma de decisiones respecto de los cambios o estrategias de fortalecimiento que se quieran lograr, resaltándose así dos componentes importantes de la mejora continua: el monitoreo y el ajuste.

2.3.12 Aumento de la productividad

Con la implementación de un SGSI automatizado, luego de operarlo en una fase manual, se afirma que habrá un aumento del rendimiento, no obstante, en la literatura, se reporta el concepto de aumento de la productividad para hacer referencia al aspecto de rendimiento en diferentes ámbitos. Para Peñaloza [65] la innovación representa un elemento de competitividad, ya que permite un mayor ahorro en los variables involucradas en las operaciones, lo que aumenta la productividad.

Para la Oficina Internacional del Trabajo (OIT) [65], la productividad mide la relación que existe entre productos e insumos o en el aumento de los precios cuando no ha habido aumento en la producción, en sí se refiere a todos los factores que intervienen en la producción. Así mismo, se reconoce la productividad en el trabajo, la cual se define de acuerdo con la como la producción por unidad de insumo de mano de obra y tiene en cuenta el número de personas que apoyan y el tiempo destinado en horas. En suma, para medir la productividad en una organización se puede tener en cuenta tanto la producción o desempeño individual, como los beneficios en su conjunto.

En cualquier caso, el aumento de la productividad se favorece con la utilización de nuevos bienes de capital, los cambios organizativos, las nuevas competencias profesionales desarrolladas en el mismo entorno laboral o fuera de este. Por el contrario, a nivel organizacional el aumento de la productividad se ve afectado por la falta de gestión, la falta de inversión en instalaciones y equipos, la seguridad y la salud en el trabajo.

2.3.13 Reducción de Riesgos de Pérdida de Información

En el contexto de un SGSI los riesgos en primera instancia deben ser valorados considerando la probabilidad de que ocurra una amenaza y el posible impacto que se llegue a tener por la ocurrencia del evento. Esta ponderación lleva a que se clasifiquen según los riesgos: asumibles, no aceptables y críticos.

Luego de la valoración el tratamiento de los riesgos se puede dar de acuerdo con varias posibilidades, bien sea, asumiéndolo, evitándolo, transfiriéndolo o reduciéndolo, última alternativa que refiere a las medidas y controles que se implementan para disminuir la probabilidad de que ocurra un evento como la pérdida

de información o que se disminuya su impacto negativo en el contexto de la organización [66].

2.3.14 Controles para los Riesgos

Hace referencia a los mecanismos que permiten que un sistema de información sea seguro, para ello, el clave atender a aspectos como la integridad que garantiza que los datos no han sido alterados por externos; la confidencialidad de los datos; la disponibilidad para cuando las entidades autorizadas lo requieran; la autenticación, en tanto, el sistema pueda comprobar que los usuarios son quienes dicen ser; el no repudio o también llamado irrenunciabilidad que hace referencia al hecho de no poder negar la emoción o recepción de una información cuando realmente fue realizada la acción. Finalmente, es importante el control de acceso donde podrán ingresar al sistema solo el administrador o personal autorizado [67].

CAPITULO III. MATERIALES Y MÉTODOS

La presente propuesta configura una investigación aplicada que se soporta en aportes tecnológicos [18], [55], legales y de gestión de calidad como ya se vio en todo

el marco de contexto ofrecido anteriormente, así como de métodos cualitativos para ofrecer una solución al Departamento de Sistemas de una institución universitaria, contribuyendo así a la seguridad de la información desde las medidas de protección y de las exigencias que por ley deben acatar todas las organizaciones públicas y privadas.

En una investigación aplicada el objetivo es generar nuevo conocimiento a partir de la aplicación directa en la sociedad o algún sector productivo, beneficiando así el aumento del nivel de vida de la población y en la creación de oportunidades de empleo. Este tipo de investigación puede utilizar un conocimiento previo derivado de un pilotaje, una fase diagnóstica o de la investigación básica para solucionar un problema en concreto. [18]

Dentro de la investigación aplicada, la investigación tecnológica o también conocida como investigación y desarrollo tiene un espacio preponderante porque busca generar un impacto a partir de la creación de artefactos o de procesos para mejorar prácticas, hacerlas más eficientes, así como obtener beneficios económicos [18], [55]. Para el caso, la presente investigación consiste en identificar las necesidades a partir de formatos estandarizados como el de la Normas ISO/27001 y de protección de datos personales para luego sugerir una solución tecnológica bajo los parámetros propios del área articulando los requerimientos exigidos y encontrados para que el proyecto aplicado logre sus propósitos.

3.1 Lugar de ejecución

La investigación se desarrolló en una institución universitaria de carácter privado, a partir de la necesidad de mejora encontrada en el Departamento de Sistemas la cual, como ya se expresó, refiere a la automatización del SGSI mediante la Norma ISO/IEC 27001 y al cumplimiento de la Ley 1581 de Protección de Datos Personales.

La identificación del Departamento de Sistemas se dio de manera intencional por el nivel de respuesta que tenía la institución universitaria respeto de un SGSI para dar cumplimiento a la Ley 1581 de 2012 y desde el apoyo que proporciona la Norma ISO/IEC 27001. De esta manera, la técnica de muestreo hace parte de las muestras no probabilísticas.

La técnica de muestreo intencional porque se incluye el punto de vista del investigador, pero siguiendo a Espinoza [55], es posible denominar esta muestra como “de casos sumamente importantes o críticos para el problema analizado”, ya que según los autores a veces hay casos del ambiente que no podemos dejar fuera, en este caso, donde no se trabaja con personas sino con procesos, en un sistema de gestión de seguridad informática no es posible dejar por fuera la Norma ISO 27001 y estratégicamente, tampoco la Ley 1581 ya que en el problema se está plateando una articulación justamente para optimizar los procesos.

3.2 Materias primas e insumos

Para diseñar un SGSI automatizado basado en la Norma ISO/IEC 27001:2013 que permita el cumplimiento a la Ley 1581 de 2012 de protección de datos personales en el Departamento de Sistemas de una institución universitaria en Colombia es necesario tener en cuenta unos requerimientos genéricos, funcionales y finales.

3.2.1 Requerimientos Genéricos

- Permiso de las directivas de la institución de educación superior.
- Acceso a los procesos de seguridad del Departamento del Sistemas.

3.2.2 Requerimientos Funcionales

- Conocimiento de los requerimientos propuestos por la Norma ISO/IEC 27001:2013 y exigidos por la Ley 1581 de 2012.
- Gestión del software Eramba Community para posibilitar el diseño del SGSI.
- Equipo humano del Departamento de Sistemas.

3.2.3 Requerimientos Finales

- Puesta en producción del sistema de seguridad de la información.
- Capacitación al equipo directivo acerca del uso del sistema de seguridad de la información automatizado.
- Capacitación a los departamentos involucrados con la seguridad de la información de la institución de educación superior: Jurídica, Personal, Logística y Sistemas.

3.3 Equipos y materiales

A continuación, se describe el recurso humano y tecnológico que se requiere para el diseño del sistema de gestión de la seguridad de la información en el Departamento de Sistemas de una institución de educación superior.

4.3.1. Humanos

El desarrollo de la propuesta aplicada tiene como responsable principal al investigador que aparece como autor de la investigación y al equipo técnico del Departamento de Sistemas. Por tanto, los esfuerzos que permitirán que el objetivo general se cumpla, son:

- Jefe del Departamento de Sistemas.
- Analista de Conectividad
- Analista de Infraestructura TIC
- Ingeniera Administradora del Sistema de Información.

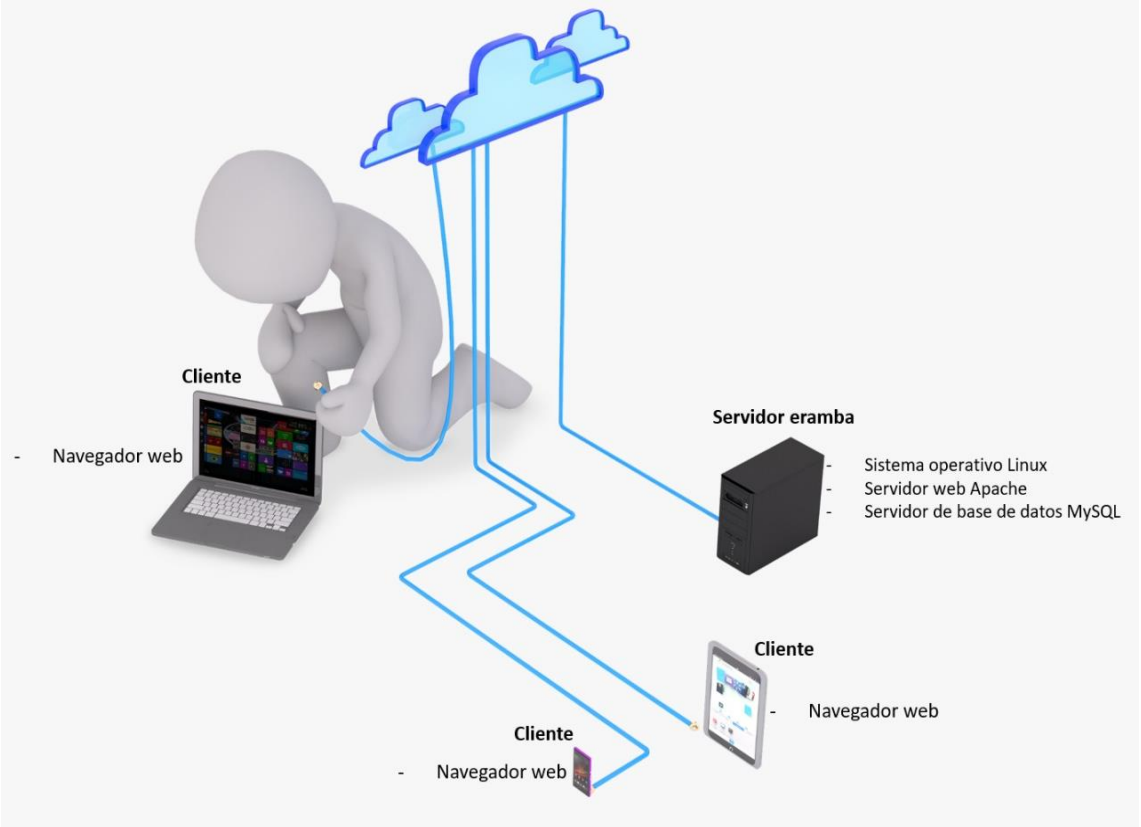
4.3.2. Tecnológicos

A nivel tecnológico, el sistema Eramba trabaja con arquitectura cliente – servidor, la cual está compuesta por un servidor con sistema operativo Linux, sistema Apache como servidor web y MariaDB como servidor de base de datos.

Para acceder a todas las funcionalidades del sistema los clientes se conectan a Eramba a través de un navegador web por medio del protocolo *http*, puede ser instalado y accedido a través de una nube pública o solo por medio de una nube privada.

Por su parte, la seguridad del sistema la garantiza el aseguramiento del sistema operativo pues se dejan abiertos solo el puerto que permite tanto la comunicación del protocolo http como el puerto que permite la comunicación *SSH* para su respectiva gestión y la configuración. Eramba tiene como medida de seguridad la gestión de usuarios autorizados que son configurados por medio del usuario administrador.

Figura 3. *Arquitectura cliente-servidor del Sistema Eramba*



Nota. Adaptación a partir de imagen obtenida del banco de pixabay y el Manual de instalación de Eramba.

A continuación, en la Tabla 4 se relacionan los costos en los que tendría que incurrir una organización que considere el diseño desde cero de un sistema de gestión de la seguridad de la información. En el caso particular no hubo una inversión adicional porque se usaron los recursos de la universidad tanto tecnológicos como humanos.

Tabla 8. *Costos por concepto de recursos tecnológicos*

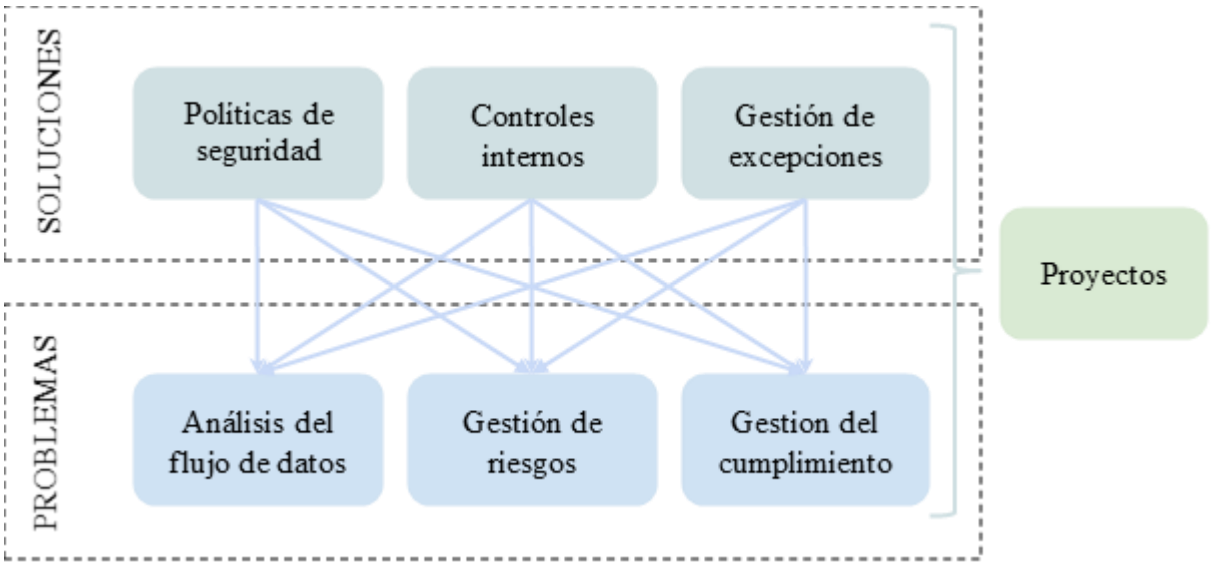
Recurso tecnológico	Costo (USD)
• Software Eramba Community	0

• Servidor con las siguientes características: Memoria ram 4 gigas Procesador de 4 nucleos Sistemas operativo Linux Almacenamiento en disco duro de 500 gigas Servidor web Apache Servidor de base de datos MariaDB Versión PHP 7.0 o superior	3000 (anuales)
• Cuatro computadores para el equipo técnico	3500
• Servicio de internet dedicado	200 (mensual)
• Integración con sistemas de información	1000 (único pago)
• Parametrización del sistema	1500 (100 horas)
Total	9200

4.3.1 Análisis

El desarrollo del informe enfocado hacia el diseño de un sistema de seguridad de información soporta su análisis en el marco lógico que ofrece la herramienta tecnológica Eramba Community, la cual opera bajo un modelo de soluciones y problemas como se puede observar en la Figura 1.

Figura 4. *Marco lógico de la herramienta Eramba Community*



Dentro de la lógica de Eramba Community los problemas se entienden como:

- Gestión de cumplimiento: los requerimientos que se necesitan para mostrar el cumplimiento del Payment Card Industry - Data Security Standard o PCI-DSS por sus siglas en inglés.
- Gestión de riesgos: Análisis de riesgo o problemas conocidos.
- Análisis de flujo de datos: métodos para la protección de los datos.

Por su parte, dentro de las soluciones, estas aparecen una vez se entienden los problemas. De esta manera es posible adoptar la mejor solución que aparecen de:

- Las políticas de seguridad.
- Los controles internos
- La gestión de la excepción

En este sentido, la propuesta de Eramba Community indica que tanto los problemas como las soluciones pueden resultar beneficiadas en un proyecto por su mutua interrelación. Lógica que ofrece una propuesta asequible sobre el entendido de que no hay razón para diseñar e implementar soluciones costosas si sus

problemas no están bien definidos. No obstante, en la mayoría de los casos, sugiere la herramienta, es posible agrupar los problemas para resolverlos a partir de una única solución.

Ahora, la interrelación de problemas y soluciones operan según el siguiente proceso que ayuda a entender la forma en cómo se enfrentan los problemas y el papel de las soluciones en cada uno:

- Definir todos sus problemas.
- Piensa en las soluciones que existen.
- Vincular los problemas y las soluciones.

Frente a lo anterior, cabe resaltar que frente a los problemas que presentan las organizaciones, de las cuales ya tienen conocimiento, las soluciones dependen de factores sobre todo internos relativos a las ganas de querer dar solución al problema, de lo contrario, ninguna solución podrá ser bien recibida. En este caso, como recurso se utilizan las "excepciones" para dar cuenta de la situación, resaltando el momento en el que se tomó la decisión y la persona responsable de ella, así como cuándo y por quién fue aceptada.

3.4 Definición y medición de variables

Las variables del estudio resultan de los planteamientos axiológicos de la propuesta y se operacionalizan como se observa en la Tabla 2 una vez se distinguen las dimensiones y los indicadores correspondientes a cada variable, dependiente e independiente. Así mismo se delimitan los instrumentos que permitieron la recolección de información.

Tabla 9. *Operacionalización de variables*

Variable	Dimensiones	Indicadores	Operacionalización	Instrumentos
Independiente: Automatización del SGSI basado en la Norma ISO/IEC 27001:2013	Diseño y automatización del SGSI basado en la ISO/ IEC 27001:2013	• Optimización de procesos • Optimización de tiempo • Optimización de costos • Mejoramiento continuo • Aumento de la productividad	• Identificación de los requerimientos de la Norma ISO/IEC 27001:2013 • Estructuración del sistema de SGSI basado en las necesidades de la institución • Montaje e implementación del SGSI en la herramienta tecnológica	• Matriz de SGSI • Matriz de riesgos • Herramienta Tecnológica Eramba Community
Dependiente: Cumplimiento de la Ley 1581 de 2012	• Cumplimiento de la Ley 1581 de 2012 de protección de datos personales • Optimización y seguimiento del SGSI en el Departamento de Sistemas de la institución universitaria	• Optimización de costos • Optimización en la demostración del cumplimiento de la Ley • Reducción de riesgos de pérdida de información • Controles para los riesgos	• Identificación de bases de datos con información personal • Clasificación de datos	Matriz de cumplimiento de la Ley 1581 de 2012 con nivel de cumplimiento

3.5 Métodos de análisis / Evaluación

La recolección de los datos sigue los procesos desarrollados por la Norma ISO/IEC 27001, la Ley 1581 y la evaluación final del diseño bajo criterios técnicos. La identificación inicial de la problemática se apoya en la técnica de observación participante, la cual hace referencia según Jociles [68] a un ejercicio en el cual el investigador interviene con su presencia y observación en el contexto de interés.

Dicho de otro modo, la observación participante no es una observación a distancia, sino por el contrario da cuenta de la relación entre quien investiga y los sujetos-objetos [69] en el escenario que les es propio. Técnica que se apoyó de la estructura de un diagnóstico para organizar las observaciones realizadas en el Departamento de Sistemas de la Institución Universitaria.

El registro de los datos observados se apoyó de instrumentos como la guía de observación y listas de cotejo. De acuerdo con Campos y Lule [70], el primer instrumento le permite al investigador, en el ejercicio de observación, tanto ubicar la atención de una manera sistemática en los aspectos relacionados con el objeto de estudio, como registrar los datos procedentes de tal acción. En el caso particular, la guía de observación permitió registrar los aspectos clave a evaluar en el proceso de automatización mediante la Herramienta Tecnológica Eramba Community.

En cuanto a la lista de cotejo, estas hacen referencia a un listado de aspectos a evaluar la cual incluye un puntaje y una observación que permite la construcción de una línea base [71]. Este instrumento se nutrió con los datos procedentes de la guía de observación, respaldando el diagnóstico del SGSI y sustentaron desde luego la evaluación.

Como instrumento, las listas de chequeo permitieron evaluar el nivel de cumplimiento tras la implementación de un SGSI, se identificó el riesgo de acuerdo con las escalas de probabilidad e impacto atendiendo a la Norma ISO 27001 y el cumplimiento de la Ley 1581 de 2012.

3.6 Diseño de Investigación

La investigación desde el enfoque aplicado que se propone presenta un carácter experimental, ya que se plantea la automatización de un proceso para mejorar la

eficiencia de la respuesta y la calidad del mismo [55]. En este sentido, se están manipulando intencionalmente unas variables independientes para analizar sus consecuencias sobre las variables dependientes dentro del ejercicio controlado en el Departamento de Sistemas de la institución universitaria.

La línea base de la propuesta se construye a partir del diagnóstico propuesto como primer objetivo específico y aunque la investigación no presenta un alcance evaluativo, tras la implementación del SGSI en el software de código abierto Eramba Community [53] se presentan las ventajas y desventajas que presenta la automatización para responder con el cumplimiento de la Ley de protección de datos. Luego, se avanzó hacia el desarrollo de la investigación para dar cumplimiento a los objetivos y finalmente se evaluó el proyecto de manera interna y desde la mirada de expertos en el área.

CAPÍTULO IV. PROPUESTA DE INGENIERÍA

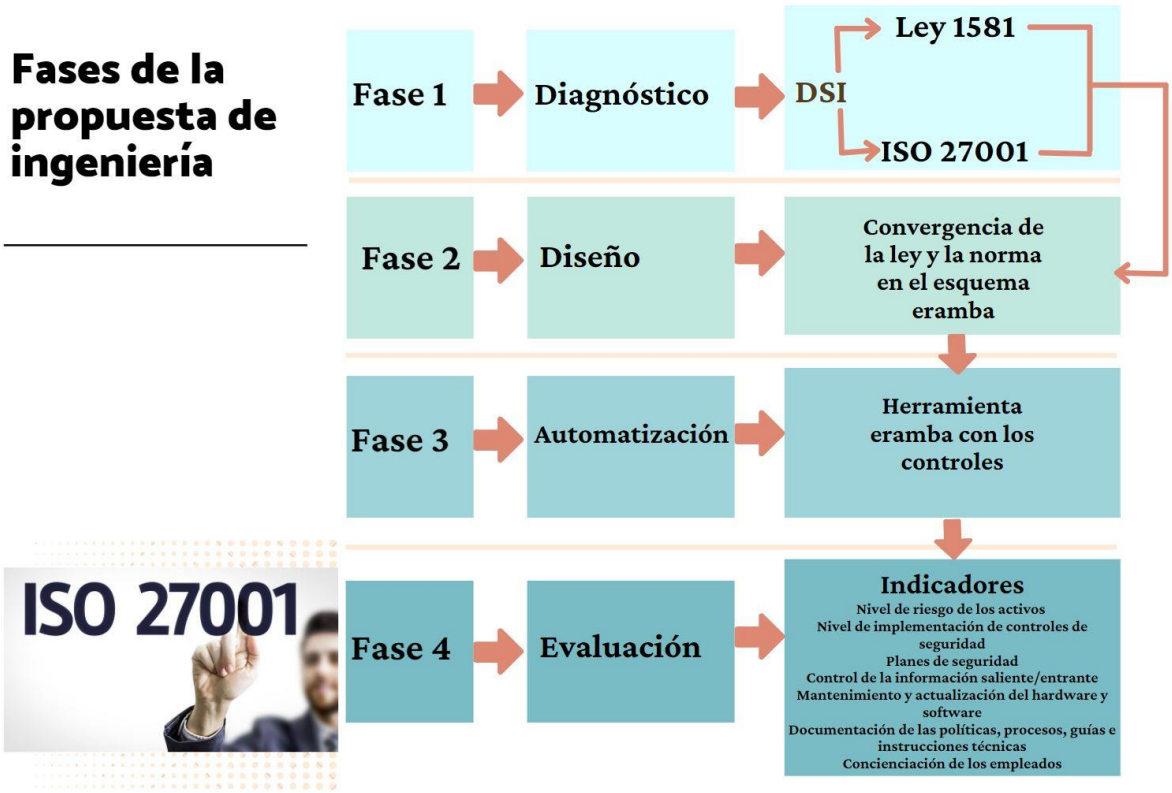
El informe presentó un alcance aplicado al área de la gestión de la seguridad de información en el Departamento de Sistemas de una institución universitaria, el cual busca diseñar un SGSI para articular de manera automatizada la Norma ISO/IEC 27001 con la Ley colombiana de Protección de Datos Personales 1581 que mejores los procesos de seguridad de información.

De acuerdo con lo anterior, se entiende que el ejercicio de trabajo aplicado llega hasta el diseño del SGSI automatizado y no a la implementación y puesta en marcha del sistema de seguridad. Sin embargo, aunque el alcance de la investigación no propone un seguimiento a la implementación del sistema y mucho menos una evaluación del proceso, si se realiza un ejercicio evaluativo para reconocer las mejoras que se proporcionan a partir del diseño del SGSI. Aspectos puntuales de la herramienta se identificarán y mejorarán durante el tiempo de implementación de la propuesta.

De esta manera, la delimitación del alcance permite abordar la ruta de acción soportada en los objetivos específicos, desde los cuales se procedió como se indica a continuación:

1. El diagnóstico se realizó al visualizar el cumplimiento del DSI respecto de las exigencias de la Ley 1581 de 2012 y la respuesta que organizativamente se podían dar desde la Norma ISO/IEC 27001.
2. Con el insumo del punto anterior se condensaron las pautas para el diseño del sistema atendiendo a las particularidades y convergencias planteadas por la Norma y la Ley, el cual se adaptó al esquema propuesto por la herramienta Eramba.
3. La herramienta Eramba permitió la automatización del SGSI, ya que cuenta con recursos como los controles necesarios para la protección y gestión de la información y el monitoreo de cumplimiento. Además, al ser de acceso abierto, herramienta permite el logro de este tipo de objetivos a bajo costo.
4. Tras la automatización del SGSI la plataforma está disponible y operando conforme a las finalidades, no obstante, dado que el alcance de la investigación no consideró una implementación y posterior evaluación del proceso, se consideró necesario ofrecer unos elementos que, a modo de medición, permitieran comparar los resultados una vez integrado este nuevo recurso al DSI. Dicho ejercicio tuvo en cuenta los indicadores de la medición de riesgo atendidos durante el diagnóstico y otros sugeridos para las evaluaciones del tipo de sistema de gestión abordado, cuya línea base de estos últimos se atendió desde la no existencia contrastado con los beneficios actuales.

Figura 5. *Fases de la propuesta de ingeniería*



CAPITULO V. RESULTADOS Y DISCUSIÓN

5.1 Diagnóstico acerca de los Procedimientos Realizados para la SGSI

Este numeral ofrece un diagnóstico acerca del cumplimiento que la institución universitaria de estudio tiene frente a la Norma ISO 27001 y propiamente con la Ley 1581. Se indica así mismo el cumplimiento frente al Registro Nacional de Bases de datos, cómo es posible cumplir la Ley a partir de la articulación con la Norma, un análisis de riesgo y el estado de la aplicación de controles de seguridad de la información. En suma, el diagnóstico permite analizar cómo ha sido la gestión de la calidad de la Universidad en tanto el cumplimiento a las disposiciones mencionadas.

5.2.1 Diagnóstico a Partir de los Requisitos de la Norma ISO 27001

En consideración con los requisitos que exige la Norma ISO 27001 para su diseño e implementación, el diagnóstico que realizó el Departamento de Sistemas e Informática (DSI) partió de la evaluación que se muestra en el Anexo 3 para identificar el nivel de cumplimiento. Para ello, se revisó cada requerimiento con el equipo técnico de tecnología de la información, haciendo un análisis de lo que al momento se tiene se tiene en relación con lo que se exige.

Los resultados muestran en la Tabla 11 que existe un cumplimiento del 11% frente a un incumplimiento de requisitos en el 63% y un 26% con esfuerzos en un nivel inicial. Estos hallazgos que por un lado se convierten en el punto de partida del desarrollo metodológico y por otro, justifican la necesidad de diseñar formalmente el SGSI propuesto por la Norma ISO 27001, al menos dentro del DSI de la universidad de estudio.

Tabla 10. *Estado de implementación del SGSI basado en la Norma ISO 27001 en el DSI de la Universidad Contexto de Estudio.*

Nivel	Significado	Estado de la implementación SGSI
Desconocido	No ha sido verificado	**0%**
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.	**63%**

Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.	**26%**
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.	**0%**
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.	**7%**
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.	**4%**
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.	**0%**
No aplicable	A fin de certificar un SGSI, todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.	**0%**
	Total	100%

5.2.2 Diagnóstico a partir de los requisitos de la Ley 1581 de 2012

Para el diagnóstico bajo los requisitos de la Ley 1581 de 2012, la evaluación igualmente midió el avance, pero esta vez ya no de diseño e implementación sino de

cumplimiento de los principios y deberes (véase anexo 3), encontrándose que de los 86 principios y deberes el DSI solo cumple con el 43% (ver Tabla 12).

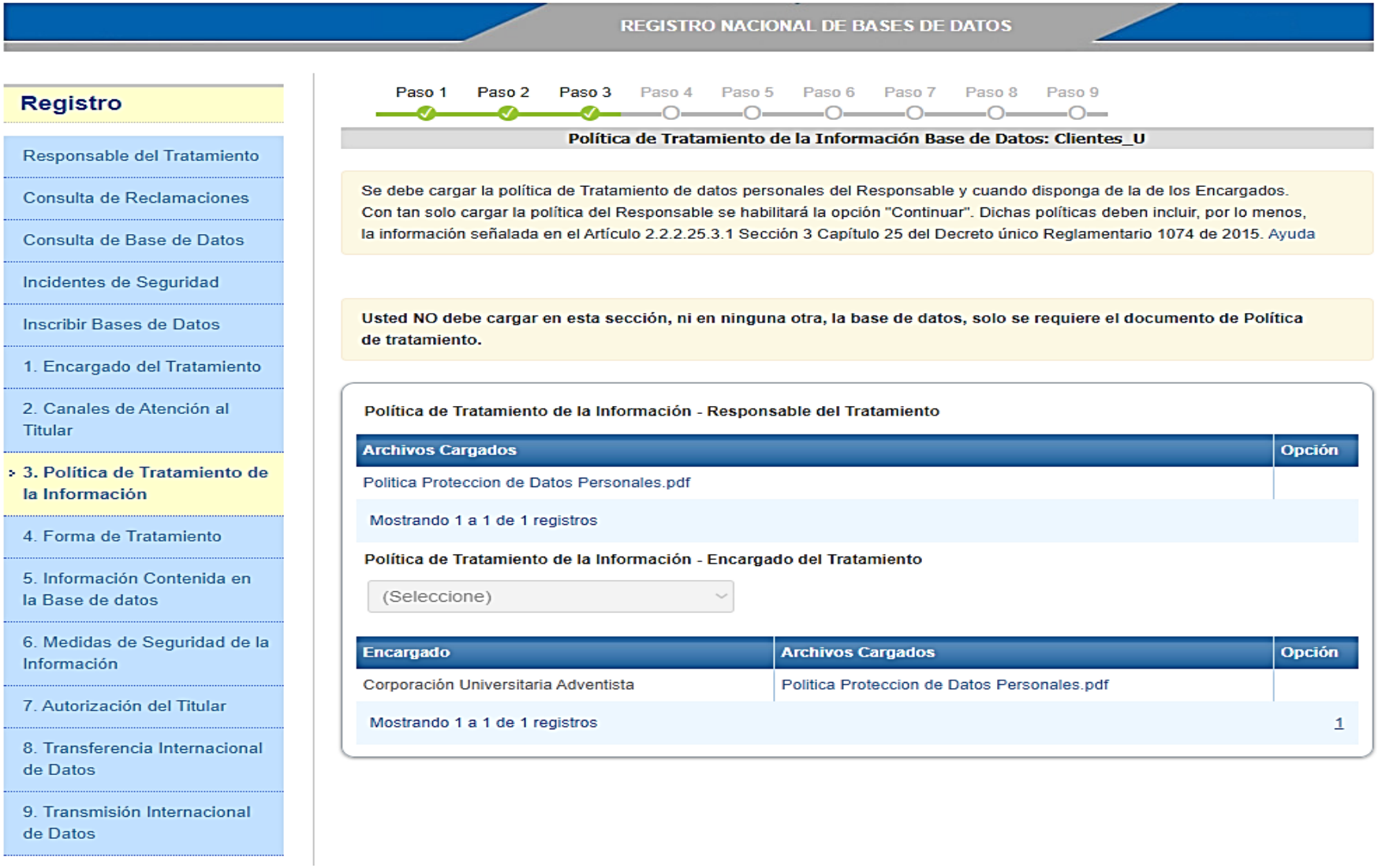
Tabla 11. Porcentaje de cumplimiento según los principios y deberes de la Ley 1581 - DSI

Estado	Significado	Comprobación cumplimiento principios y deberes Ley 1581 - DSI
NO CUMPLE	El requisito de la Ley 1581 "NO" se encuentra articulado con la Norma ISO 27001	**57%**
SI CUMPLE	El requisito de la Ley 1581 "SI" se encuentra articulado con la Norma ISO 27001	**43%**
No aplicable	No aplica	**0%**

5.2.3 Registro Nacional de Bases de Datos RNBD

Derivado de La ley 1581 para la protección de datos, otra medición del nivel de avance corresponde al Registro Nacional de Bases de Datos (ver Figura 4), el cual es un proceso que se debe realizar ante la SIC a través de su portal de registro y pide 25 requisitos adicionales.

Figura 6. Registro Nacional de Bases de Datos RNBD



Considerado este requerimiento adicional de registro ante el RNBD, el DSI se propuso incluirlo como parte del diagnóstico para verificar el nivel de cumplimiento de los requisitos exigidos. Los resultados indican que de los 25 requisitos hay un cumplimiento del 28%, frente a un 64% de incumplimiento y un 8% que no aplica (véase Tabla 13).

Tabla 12. Porcentaje de cumplimiento según los requisitos de la Ley 1581 RNBD

Cumplimiento	Significado	Cumplimiento de los requisitos de 1581 RNBD
NO CUMPLE	No se cumple el requisito	**64%**
SI CUMPLE	Se cumple el requisito	**28%**
NO APLICA	No aplica	**8%**
	Total	100%

5.2.4 Verificación de Requisitos de la Norma ISO 27001:2013 para cumplir la Ley 1581

Luego de verificar el nivel de cumplimiento por parte del DSI de las cláusulas de la Norma ISO 27001:2013 y los requisitos de la Ley 1581, se procede a analizar si la Norma ISO es suficiente para dar cumplimiento a los requisitos que exige el estado colombiano a través de la Ley.

En la Tabla 14 se presenta un resumen luego de cotejar las cláusulas y controles de la Norma ISO 27001:2013 para verificar cuáles permitían el cumplimiento de la Ley 1581 (ver Anexo 4) de acuerdo con el primer listado de requisitos correspondiente a los principios y deberes, la cual indica que existe un cumplimiento del 100%, lo que respalda la propuesta de articular la Ley 1581 con la Norma ISO 27001.

Tabla 13. *Resumen ISO cumpliendo requisitos de la ley 1581*

Estado	Significado	Relación Ley 1581 ISO 27001 Cumplimiento
NO ISO 27001	El cumplimiento de la Ley 1581 "NO" se encuentra articulado con la Norma ISO 27001	**0%**
SI ISO 27001	El cumplimiento de la Ley 1581 "SI" se encuentra articulado con la Norma ISO 27001	**100%**
NO APLICABLE	No aplica	**0%**

Con base en la metodología que se implementó para analizar el listado de cumplimiento de la Ley 1581, se concluye que la Norma ISO 27001 cumple todos los requisitos que la Ley exige, sin embargo, como parte del diagnóstico se presenta importante complementar este resultado con un análisis de riesgos del DSI, mismo que se hace necesario para el diseño del SGSI.

5.2.5 Resultados del análisis de riesgos

Como resultado del análisis de riesgos, donde se asignó un nivel de amenaza a los activos del DSA, se encontró que las amenazas que superan el valor 4 de riesgos están relacionadas con el suministro eléctrico como se observa en la Tabla 15, los cuales deben ser atendidos por parte del DSI, así como las amenazas que se encuentran en el límite de 4 e incluso los que aparecen en el nivel de riesgo 3.

Tabla 14. Resumen de análisis de riesgos

RESÚMEN DE ANÁLISIS DE RIESGOS					
Activo		**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Computadores y servidores (web, BD, archivos, dominio, DNS)	C1	Corte del suministro eléctrico	Medio (2)	Alto (3)	6
Sitio web y redes sociales que gestionan desde la empresa	C5	Corte del suministro eléctrico	Medio (2)	Alto (3)	6
Herramientas para empresas en la nube (G Suite, Office 365)	C6	Corte del suministro eléctrico	Medio (2)	Alto (3)	6

Firewall y Switches	C7	Corte del suministro eléctrico	Medio (2)	Alto (3)	6
Software	C8	Corte del suministro eléctrico	Medio (2)	Alto (3)	6

5.2.6 Estado y Aplicabilidad de Controles de Seguridad de la Información

Luego de haber realizado el análisis de riesgos en el DSI se procede a realizar el estado de aplicabilidad de los 114 controles de seguridad de la información que aparecen en el Anexo A (ver Anexo 5) de la Norma ISO 27001:2013. En resumen, la Tabla 16.

Tabla 15. Análisis de riesgos en el DSI

Estado	Significado	Proporción de Controles de Seguridad de la Información
Desconocido	No ha sido verificado	**91%**
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.	**4%**
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte	**1%**

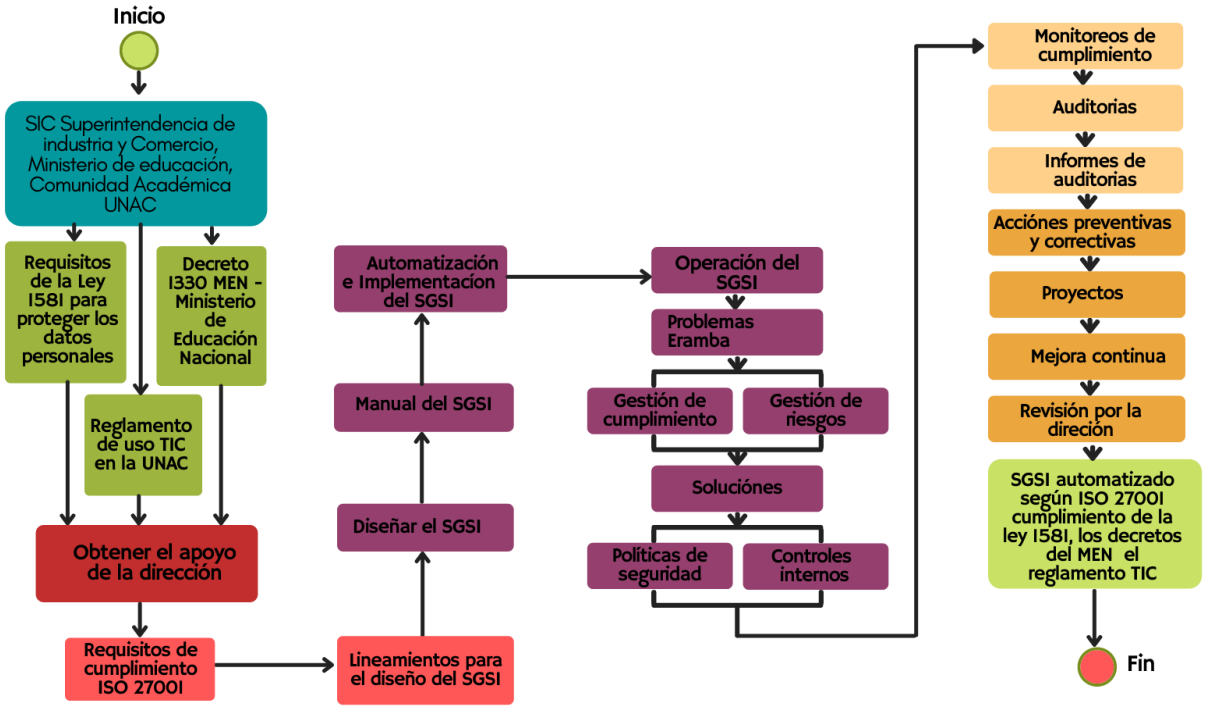
	y de tener personal de la alta calidad.	
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.	**0%**
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.	**3%**
Administrado	El control se lleva a cabo de acuerdo con un procedimiento documentado, aprobado y formalizado.	**0%**
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.	**0%**
No aplicable	A fin de certificar un SGSI, todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.	**1%**

5.2 Diseño del sistema que integre de los requisitos de la Norma ISO/IEC 27001:2013 con las exigencias impuestas por la Ley 1581 de 2012

El diseño para la articulación de la Norma ISO/IEC 27001:2013 y el cumplimiento de la Ley 1581 de 2012 (que expone las condiciones para la protección de datos) como paso previo a la automatización mediante la aplicación web Eramba Community, la cual se usa para la gestión del riesgo de cumplimiento, tuvo en cuenta los requerimientos tanto de la Norma como los requisitos de la Ley, así como los componentes del modelo que propone la aplicación web y el proceso propio del desarrollo del sistema, a fin de

que el diseño quede operable y posteriormente sea implantado[2] en el Departamento de Sistemas de la universidad contexto de la investigación.

Figura 7. Diseño del sistema integrado



El diseño que se observa en la Figura 5 incluye:

- Los componentes de la Norma ISO/IEC 27001:2013 que incluye los 27 requisitos de cumplimiento que se encuentran en los numerales 4 al 8 de la Norma (ver Tabla 10) y los 114 controles del Anexo A (ver Anexo 5).
- Los componentes de la Ley 1581 de 2012 son 86 requisitos (ver Anexo 1).

[2] La implantación no está incluida dentro de los alcances de la investigación.

- Los componentes del modelo de soluciones y problemas de Eramba Community, que como herramienta de automatización del gobierno, riesgo y cumplimiento se gestiona a través de problemas permitiendo identificar los requisitos de cumplimiento y los riesgos a gestionar. Al identificar los problemas, Eramba Community da las soluciones a través de las políticas de seguridad y los controles internos.

Conforme con los requisitos de la Norma y la estructura que ofrece Eramba Community, las etapas del diseño e implementación del sistema de gestión de la seguridad de la información SGSI tuvieron como eje principal el ciclo de mejora continua de ISO PHVA identificadas en el modelo y descritas a continuación:

- Identificar las partes interesadas y los requisitos legales
- Obtener el apoyo de la dirección
- Definir los requisitos y controles de la Norma ISO 27001 a cumplir
- Diseñar el SGSI
- Crear el SGSI
- Automatizar el SGSI con un sistema informático (Eramba Community).
- Operar el SGSI a través de Eramba Community.
- Eramba Community opera el SGSI definiendo los problemas, que para el caso de ISO 27001 son los requisitos de cumplimiento y los requisitos de cumplimiento de la Ley 1581.
- Se definen los riesgos a gestionar de acuerdo al Anexo A de ISO 27001.
- Eramba Community opera el SGSI a través de las soluciones a los problemas, que para el sistema se agrupan en los paquetes de cumplimiento que son los

requisitos de la Norma ISO 27001:2013 y los requisitos de la ley 1581 de protección de datos personales, mediante las políticas de seguridad y los controles internos.

- Eramba Community permite hacer monitoreo a las políticas de seguridad y los controles internos.
- Eramba Community permite gestionar las auditorías y generar los informes de auditoría.
- De las auditorías se identifican las acciones preventivas y las acciones correctivas que en Eramba Community son gestionadas a través de los proyectos.
- Los proyectos permiten gestionar la mejora continua del SGSI.
- La mejora continua genera el ciclo PHVA que es el núcleo del SGSI.
- Luego de definir las mejoras continuas se genera el informe de la dirección, el cual permite terminar de definir que el SGSI ha sido, en este caso, diseñado y automatizado gracias a la herramienta de software Eramba Community.

5.3 Automatización del sistema de seguridad de la información

Siguiendo el proceso de diseño presentado en el numeral anterior, el proceso de automatización se rige bajo la estructura del sistema Eramba Community que como función principal tiene la seguridad de la información en la gestión del cumplimiento de las Normas y leyes, análisis y gestión de los riesgos y auditorías de los controles que gestionan los riesgos de la información de cualquier organización.

En términos operativos, la funcionalidad de Eramba Community para el presente proyecto permite articular de manera automatizada los principios para el tratamiento de datos personales de la Ley 1581 con los controles que proporciona la Norma ISO 27001, siguiendo la relación que se presenta en el Anexo 2 donde al implementar la Norma se cumple la Ley.

Al llevar esta articulación al sistema para proceder con la propuesta de manera automatizada, el proceso se muestra de la siguiente forma:

En la Figura 6 se muestra el tablero de mando Eramba Community con las políticas de seguridad y los paquetes de cumplimiento ISO 27001/2013, Anexo A de ISO 27001/2013 y Ley 1581 de protección de datos personales. El tablero de mando o panel de control es la primera ventana del sistema Eramba Community que se observa una vez se ingresa al sistema y permite visualizar los paquetes de cumplimiento, las políticas de seguridad de la información y los controles del SGSI.

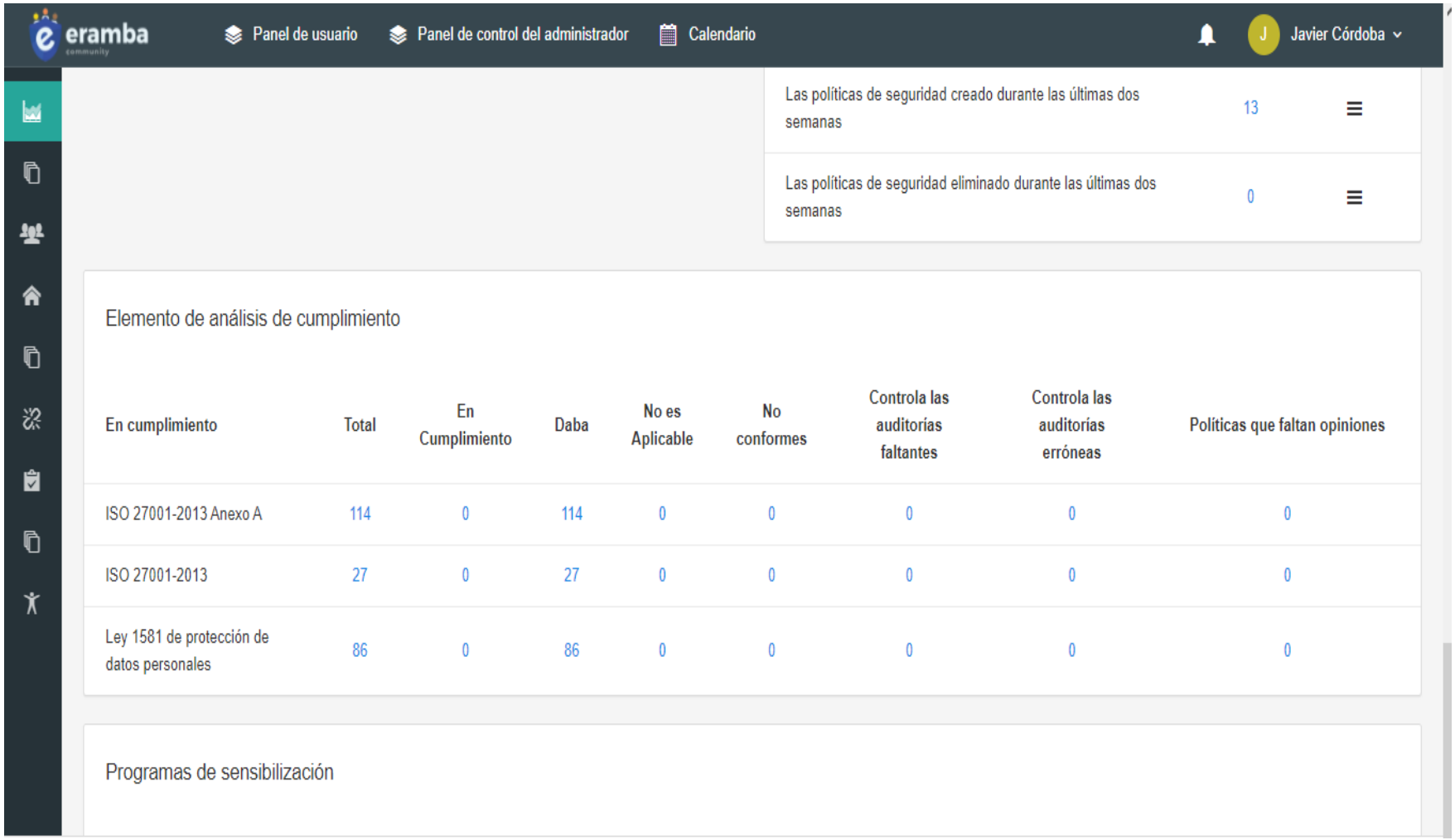
En la Figura 7 se visualizan dentro de Eramba Community los paquetes de cumplimiento los cuales están representados por el listado de 86 requisitos de la Ley 1581 de protección de datos personales y por el listado de los 27 requisitos de la Norma ISO 27001/2013 que se presentan en la Figura 8. Así mismo, por el listado de los 114 requisitos del Anexo A de la Norma ISO 27001/2013 que se visualiza en la Figura 9, los cuales se presentan como un complemento a los 27 requisitos principales.

En la Figura 10 se visualizan las políticas de seguridad de la información, las cuales son los documentos requeridos por la Norma ISO 27001/2013 y autorizados por la Alta Gerencia de la organización, que requieren una revisión periódica y ayudan al SGSI a

cumplir con las necesidades legales (Ley 1581 para e caso), regulatorias o de cumplimiento. Consecuentemente, en la Figura 11 se visualiza un portal web que proporciona acceso interno y externo a los documentos relacionados con el SGSI, cómo las políticas de seguridad, entre otros. Por su parte, en la Figura 12 se visualiza el detalle de las políticas de seguridad de la información en el cual se puede tener acceso a cada documento de las diferentes políticas en el SGSI.

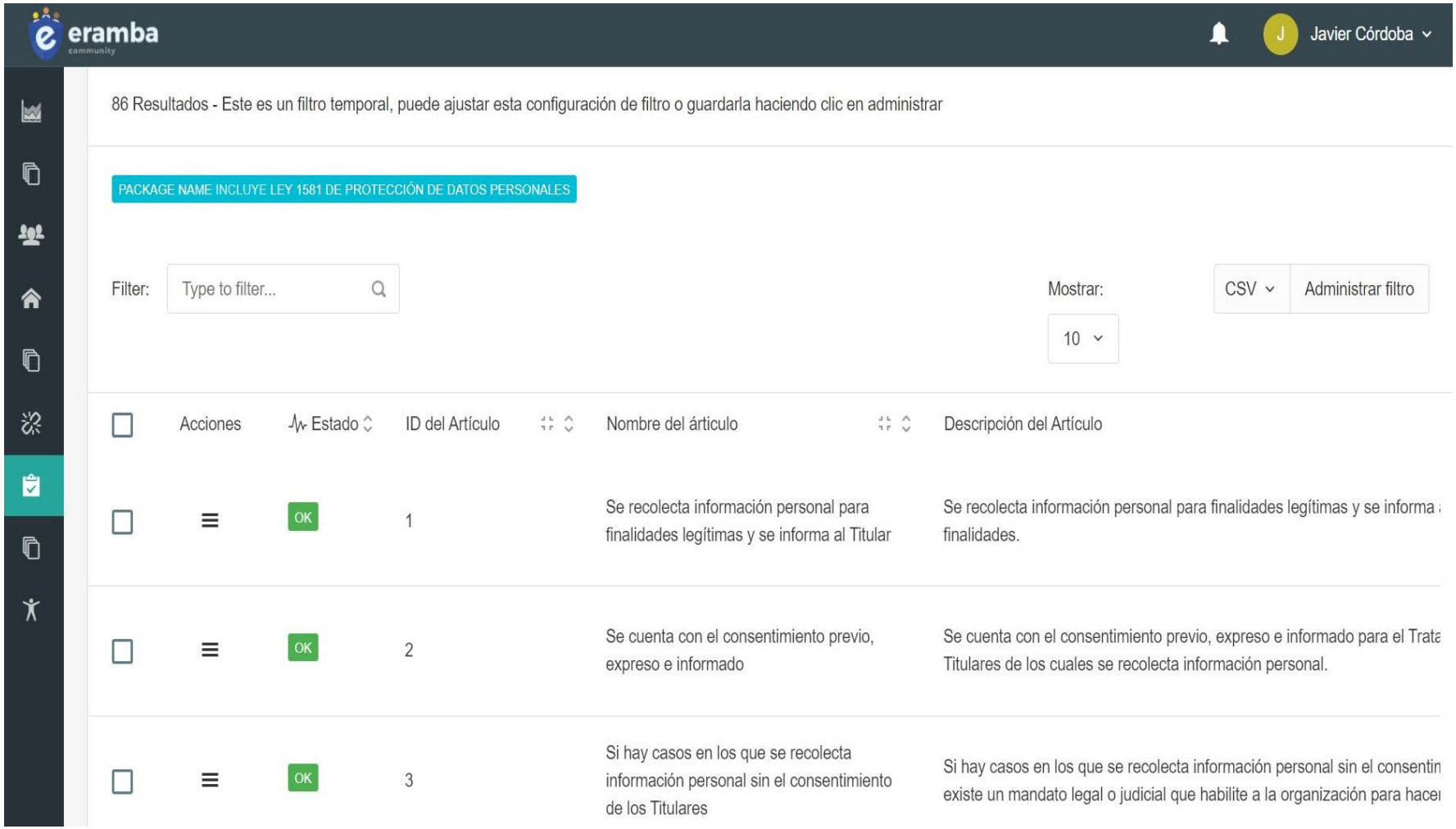
Finalmente, en la Figura 13 se visualizan los 21 controles internos, los cuales son un componente clave en el SGSI, ya que a través de ellos es posible la documentación, la evidencia de su mantenimiento y prueba.

Figura 8. *Tablero de mando de Eramba Community*



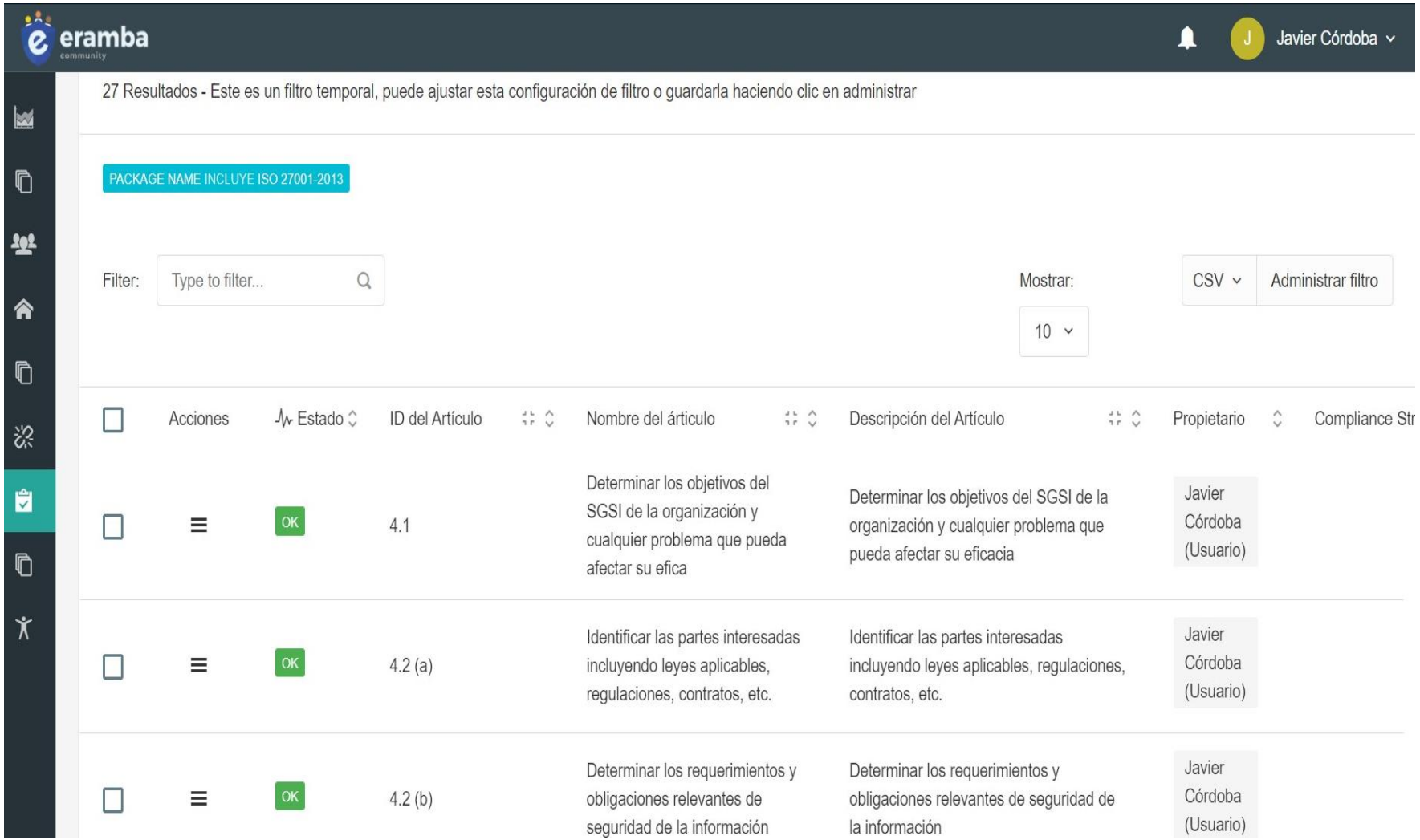
Nota. Imagen tomada de la automatización del SGSI mediante el software Eramba (2020) versión de aplicación y esquema de base de datos c2.8.1

Figura 9. *86 requisitos de cumplimiento Ley 1581 de protección de datos personales*



Nota. Imagen tomada de la automatización del SGSI mediante el software Eramba (2020) versión de aplicación y esquema de base de datos c2.8.1

Figura 10. *27 requisitos de cumplimiento ISO 27001/2013*

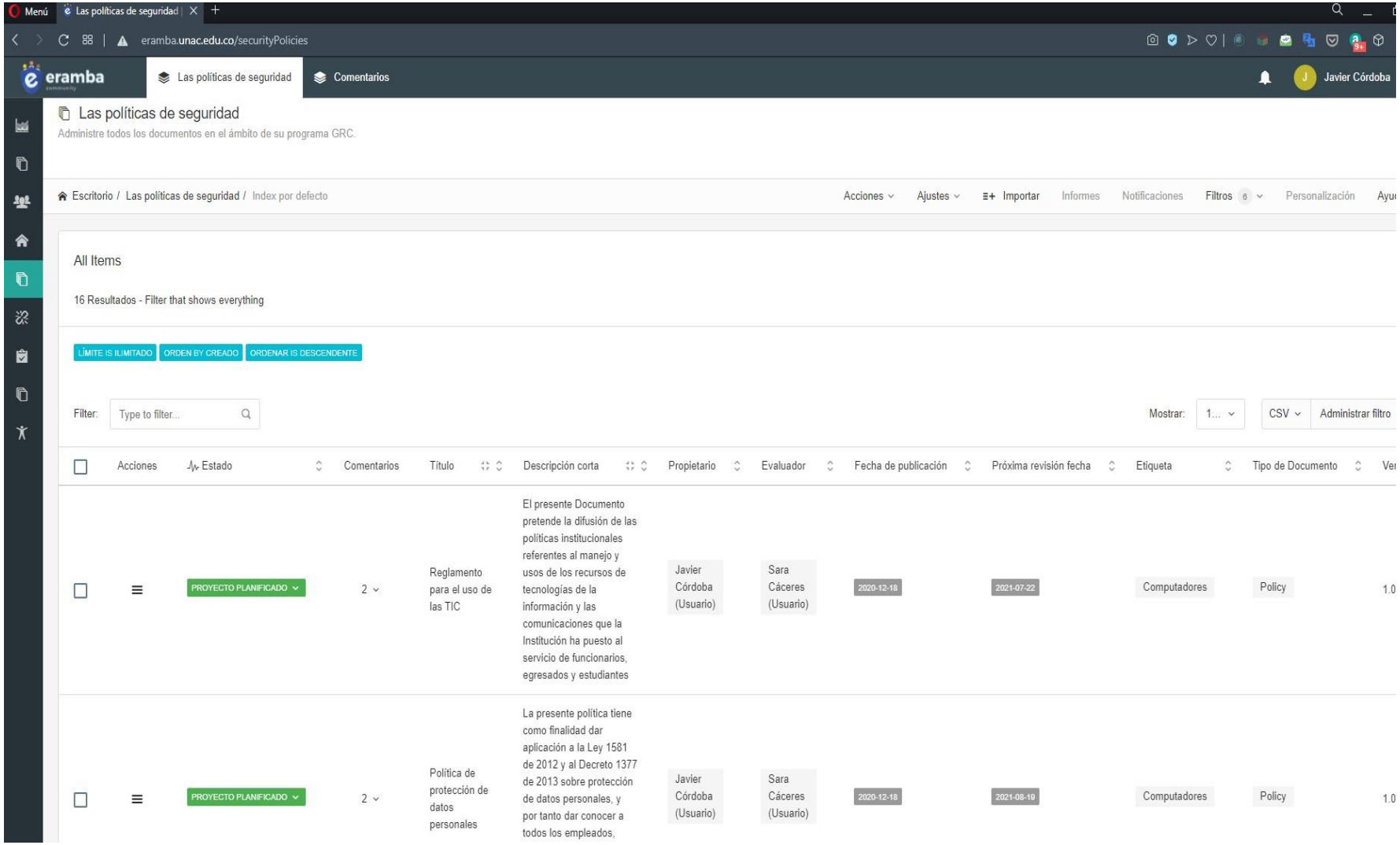


Nota. Imagen tomada de la automatización del SGSI mediante el software Eramba (2020) versión de aplicación y esquema de base de datos c2.8.1

Figura 11. *114 requisitos de cumplimiento Anexo A ISO 27001/2013*

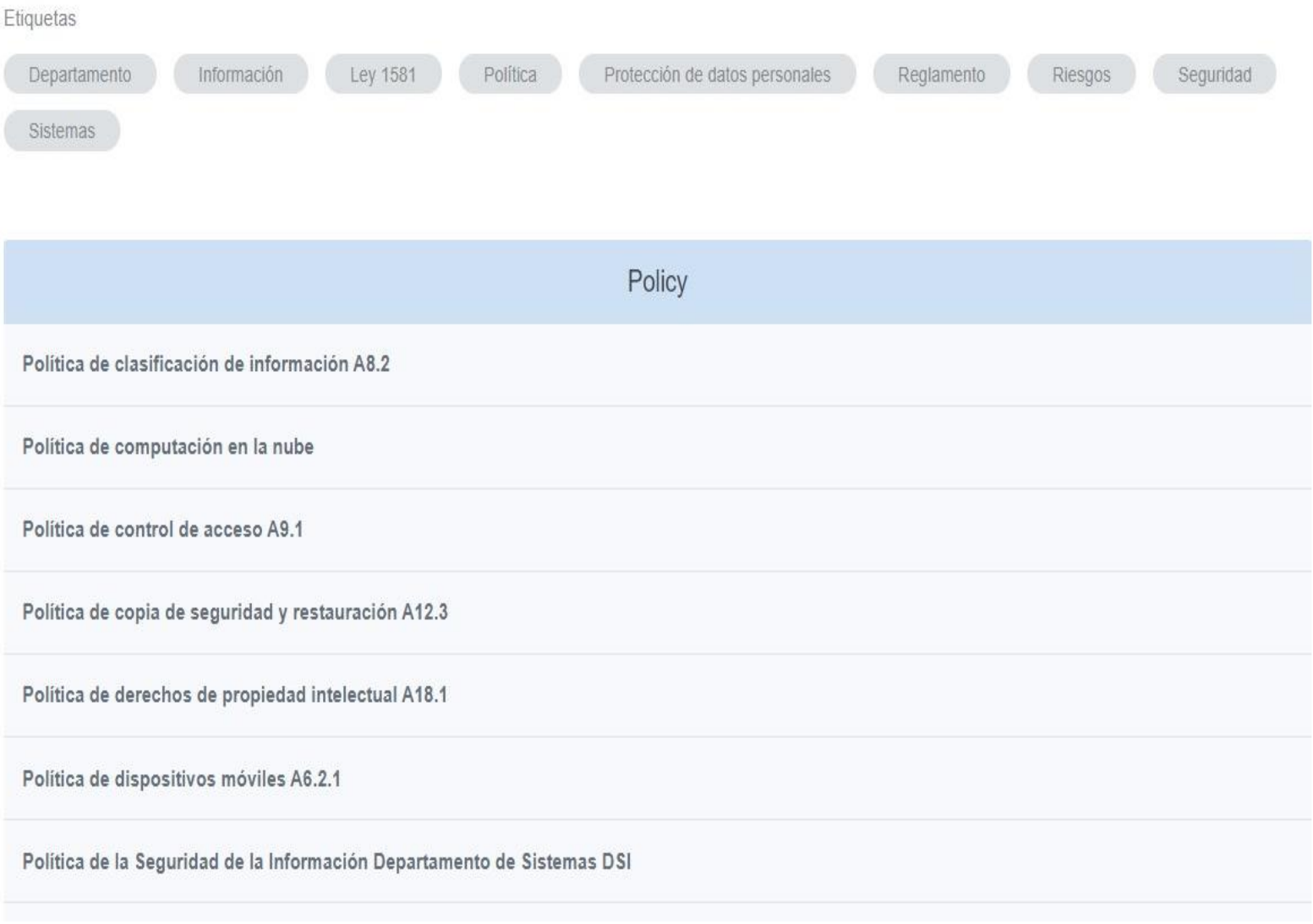
Nota. Imagen tomada de la automatización del SGSI mediante el software Eramba (2020) versión de aplicación y esquema de base de datos c2.8.1

Figura 12. *13 políticas de seguridad para dar cumplimiento ISO 27001/2013 y Ley 1581 de protección de datos personales.*



Nota. Imagen tomada de la automatización del SGSI mediante el software Eramba (2020) versión de aplicación y esquema de base de datos c2.8.1

Figura 13. *Portal de políticas*

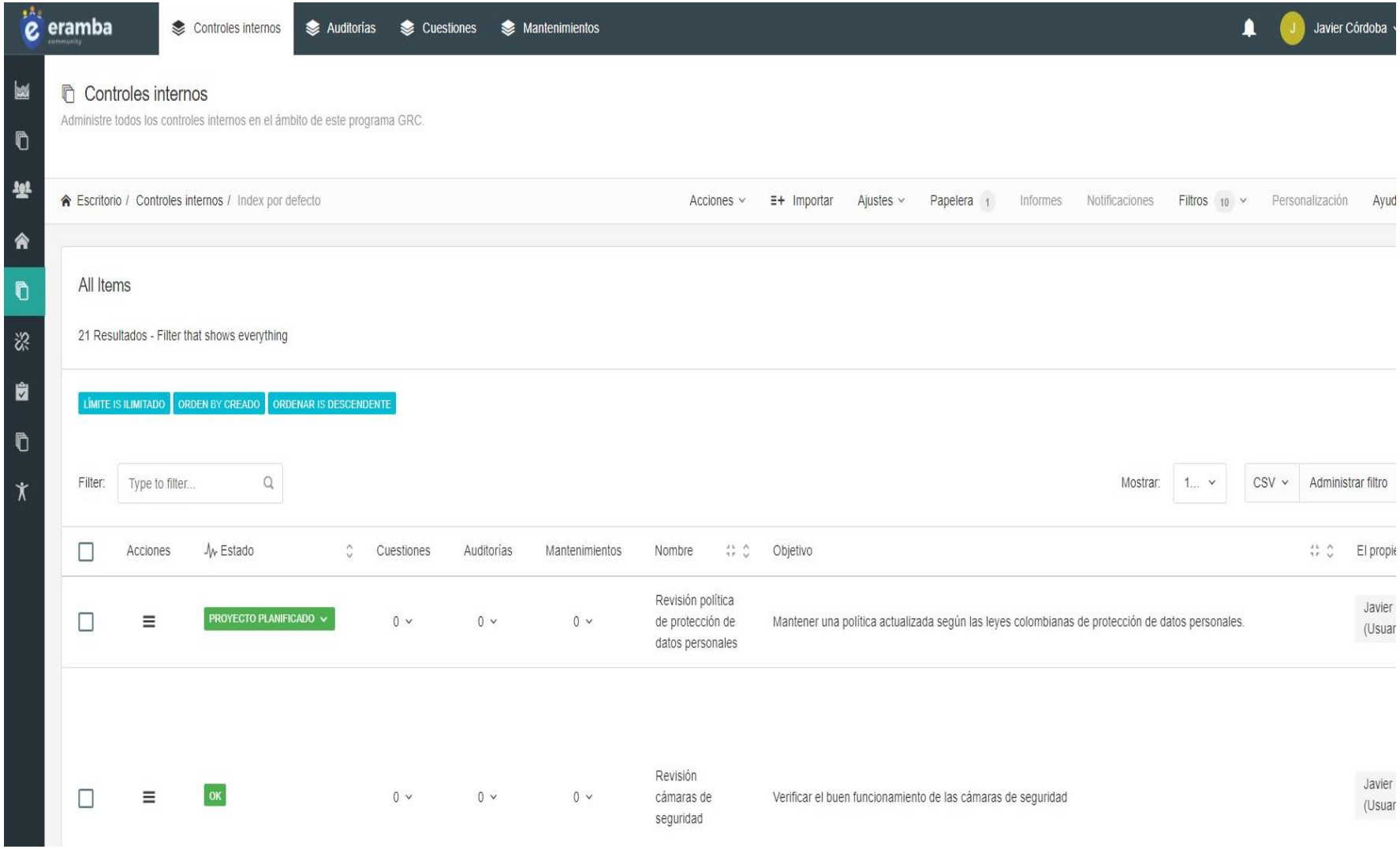


Nota. Imagen tomada de la automatización del SGSI mediante el software Eramba (2020) versión de aplicación y esquema de base de datos c2.8.1

Figura 14. *Detalle de las políticas de seguridad*

Nota. Imagen tomada de la automatización del SGSI mediante el software Eramba (2020) versión de aplicación y esquema de base de datos c2.8.1

Figura 15. *21 Controles de seguridad para dar cumplimiento ISO 27001/2013 y Ley 1581 de protección de datos personales*



Nota. Imagen tomada de la automatización del SGSI mediante el software Eramba (2020) versión de aplicación y esquema de base de datos c2.8.1

Así visto, Eramba Community se presenta como estructura lógica dinamizada por opciones ágiles que gestionan la información respetiva a la seguridad de la información de una manera intuitiva, aunque como paso previo a la alimentación del sistema requiera de un proceso paso a paso para la consecución y organización de los requerimientos, políticas, controles y estándares.

Con el diseño automatizado de un SGSI basado en la norma ISO 27001/2013 a través del sistema Eramba Community para el cumplimiento de la Ley 158:

- Se brinda protección al activo más importante de una organización, la información.
- Permite la mejora en los procesos de gestión del SGSI al hacer que estos se vuelven más eficientes, más rápidos.
- El diseño del SGSI da respuesta a los requisitos de la norma ISO 27001/2013, los requisitos del anexo A de la norma ISO 27001/2013 y los requisitos de la ley 1581 de protección de datos personales.
- La gestión de la documentación del SGSI se hace más fácil porque permite gestionar las versiones para tener las más actualizadas en operación, programar las revisiones en el sistema y que se informe a los encargados cuando se debe hacerle seguimiento, lo que permite ahorrar tiempo en ese proceso.
- A través del portal de políticas de Eramba Community se puede tener acceso autorizado a los documentos del SGSI para que las personas interesadas conozcan cómo se hacen los procesos que protegen la información.
- En el último capítulo del anexo A el A18 de la norma ISO 27001/2013, se dedica a los controles que permiten garantizar la aplicación de las leyes relacionadas con la seguridad de la información. En este caso la ley 1581 de protección de datos,

y para dar respuesta a ese control se tiene en el diseño del SGSI y publicado en el sistema Eramba Community las políticas que dan cumplimiento a dicha Ley.

- El diseño del SGSI basado en la norma ISO 27001/2013, automatizado con el sistema Eramba Community, les facilita el trabajo a los encargados de gestionar la seguridad de la información del DSI porque los tiempos de trabajo manual que se requieren al gestionar la documentación de las políticas y controles de seguridad se reducen.

5.4 Evaluación del sistema automatizado de seguridad de la información basado en la ISO/IEC 27001:2013 y la Ley 1581 de 2012.

Tras el diagnóstico, diseño y automatización del sistema de gestión de seguridad de la información para el DSI de la institución universitaria se hizo necesario incluir una fase evaluativa para visualizar los aspectos implementados y las mejoras que pueden incluirse como parte del fortalecimiento del sistema (Tabla 16).

Para tal fin se elaboró una matriz que tuvo en cuenta siete indicadores atendidos durante el desarrollo de la investigación y consideradas dentro de las evaluaciones realizadas al tipo de sistema trabajado [38]: nivel de riesgo de los activos, nivel de implementación de controles de seguridad, planes de seguridad, control de la información saliente/entrante, mantenimiento y actualización del hardware y software, documentación de las políticas públicas, procesos, guías e instrucciones técnicas y concienciación de los empleados como aspecto organizacional considerado como clave

durante el proceso de transición de un SGSI manual a automatizado por las implicaciones en el cambio de prácticas.

A partir de estos indicadores se establecieron los parámetros anteriores y actuales tras la automatización atendiendo a una medición de riesgos a partir del cálculo de probabilidad y el impacto de las amenazas encontradas durante el diagnóstico. El ejercicio permitió identificar una serie de mejoras por cada una de las amenazas sobre las cuales, como se indicó anteriormente servirán de nuevo punto de partida para continuar trabajando en el sistema.

Entre las mejoras encontradas se reconoce:

- La optimización en el nivel de acceso a la información si se tienen en cuenta el paso de una gestión manual de la información a la automatización del SGSI.
- Por el lado de los riesgos legales, estos disminuyen al lograrse un cumplimiento total de implementación del sistema.
- Con respecto a los planes de seguridad estos constituyen una guía para la gestión eficiente de la seguridad de la información que no se lograba con la gestión realizada previamente, del mismo modo.
- La automatización del SGSI permite el control de información que ingresa a los sistemas para garantizar su integridad, confidencialidad y disponibilidad.
- La mejora se presenta al pasar de una gestión manual con algunas actividades para la protección de cierta información a un sistema de gestión formal automatizado para la seguridad de la información. En este sentido, respecto de la base anterior, la mejora trae consigo amenazas tecnológicas que deben

atenderse a partir de controles con un blindaje hacia los aspectos de orden legal, no siendo así en el caso anterior cuando se carecía de la nueva estructura.

- A nivel organizacional el SGSI marca un antes y después en las operaciones referentes a la gestión de la información, por tanto, se empieza a crear una cultura de protección a la información mediada por la tecnología, lo que proporciona elementos de optimización en los procesos.

Señaladas las mejoras del SGSI automatizado, es importante decir, que Eramba, la herramienta usada para operarlo, puede fortalecerse a nivel del análisis de datos a través de otra herramienta open source llamada metabase, dado que la versión community de Eramba no permite gestionar la información de manera gráfica. Luego, con el complemento mencionado, se facilitaría la tarea sin incurrir en la compra del licenciamiento enterprise.

La anterior evaluación se realizó para efecto de validación interna de la investigación. No obstante, para complementar el ejercicio se incluyó la mirada de expertos con perfiles de Doctor en Ciencias de la Computación y Magister en Ingeniería de Sistemas, quienes ofrecieron sus conceptos a partir de seis ítems, cuatro de respuesta cerrada con escala de 0-100 donde se indagó acerca del cumplimiento del objetivo respecto de la adecuación de la Norma ISO 27001:2013 y el cumplimiento de la Ley 1581, pertinencia conceptual y técnica de la herramienta implementada del objetivo, además de dos preguntas de respuesta abierta referentes al tipo de controles que podrían agregarse o eliminar para la óptima implementación del SGSI en la institución mediante Eramba.

Como resultados, ambos expertos calificaron los cuatro primeros ítems en la calificación máxima y consideraron que no debe adicionarse ni eliminarse ninguno de los controles considerados, en razón de que los incluidos son los necesarios para el cumplimiento de la Ley 1581 (ver Anexo 6).

Tabla 16. Evaluación del sistema automatizado de gestión de seguridad de la información

	Antes de la automatización				Después de la automatización				Mejora
	Amenaza	**Probabilidad**	**Impacto**	**Riesgo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**	
Nivel de riesgo de los activos	Amenazas por desastres naturales y suministro eléctrico y de internet	Medio (2)	Alto (3)	6	Continúan las amenazas por desastres naturales, condiciones ambientales y suministro eléctrico y de internet pero se reducen las amenazas efecto de errores de los usuarios, errores del administrador, errores de configuración.	Medio (2)	Medio (2)	4	El SGSI ay a mejorar l infraestruct TIC como l servicios d virtualizaci servidores, copias de seguridad locales cor los servido de la nube
Nivel de implementación de controles de seguridad	No existía un SGSI automatizado, por tanto, no se llevaban a cabo controles de seguridad estrictos más allá de algunas acciones individuales por parte del	Alto (3)	Alto (3)	9	Denegación de servicios, robo extorsión e ingeniería social	Baja (1)	Alto (3)	3	Los riesgos legales disminuyen tener un cumplimien de implem del 100% d Ley 1581. controles d seguridad establecen manera rigurosa.

	DSI, se ajustaban a las operaciones manuale. Los riesgos informáticos eran bajos pero los riesgos legales altos.								
Planes de seguridad	No existían	Alto (3)	Alto (3)	9	• Degradación de los soportes de almacenamiento de la información. • Difusión de software dañino. • Caída del sistema por sobrecarga. • Pérdida de equipos. • Abuso de privilegios de acceso. • Acceso no autorizado.	Medio (2)	Alto (3)	6	Con el SG automatiza los planes seguridad proporcion seguridad sistema y a informació
Control de la información saliente/entrante	No existía, por tanto, se presentaba la oportunidad de fuga, introducción de falsa información, alteración,	Alto (3)	Alto (3)	9	• Fuga de información. • Introducción de falsa información. • Alteración de la información. • Corrupción de la información. • Destrucción de información.	Medio (2)	Alto (3)	6	Con el SG automatiza hay contro la informac entrante y saliente.

	corrupción, destrucción e interceptación de información.				• Interceptación de información (escucha)				
Mantenimiento y actualización del hardware y software	No era necesario porque no existía un SGSI automatizado. En términos informáticos la probabilidad de riesgo y el impacto son bajos. Sin embargo, el riesgo de su ausencia en términos de seguridad de la información es alto	Bajo (1)	Bajo (1)	1	Vulneraciones de seguridad por hardware sin mantenimiento y software desactualizado	Medio (2)	Alto (3)	6	Existe un S que exige mayor cont para dismi las vulnerabili que se pue presentar
Documentación de las políticas, procesos, guías e instrucciones técnicas	Estaba incompleta y se gestionaba manual. Por tanto se presentaban riesgos de	Alto (3)	Alto (3)	9	Desactualización de la documentación.	Bajo (1)	Alto (3)	3	Existe la documenta para respo con las disposicion legales de Ley 1581 a

	pérdida, evasión en la consulta, falta de control en la actualización.								partir de la orientacion de la Norm ISO 27001 documenta que ofrece controles d el software Eramba.
Concienciación de los empleados	No existía una cultura arraigada respecto de la seguridad de la información ya que no se disponía de un SGSI	Medio (2)	Alto (3)	6	Falta de transferencia de conocimiento sobre el manejo SGSI, ya que impediría acciones homogéneas	Medio (2)	Medio (2)	4	Con la implementa del SGSI s está construyen una cultura protección informació más allá de reconocimi de las disposicion legales, en desarrollo las operaci diarias, lo q es necesar para que la SGSI sea e

5.5 Discusión de resultados

En la intensión de diseñar un sistema automatizado de gestión de la seguridad de la información basado en la Norma ISO/IEC 27001:2013 para dar cumplimiento a la Ley 1581 de 2012 de protección de datos personales en el Departamento de Sistemas de una institución universitaria en Colombia y en esta medida contribuir a la estandarización de los procesos internos en cuanto al almacenamiento y la protección de la información de manera eficaz y eficiente, esta investigación se propuso inicialmente la identificación de las etapas de requerimiento que exige la Norma ISO 27001:2013 y la Ley 1581, esto con el fin de tener los insumos que luego sirvieron para alimentar el software Eramba Community desde donde se automatizó el proceso de cumplimiento. Con este objetivo fue posible evidenciar también las convergencias entre la Ley de protección de datos personales y la Norma enfocada a prevenir riesgos de seguridad de información; frente a lo cual se afirma tal como lo mencionan Venegas y Pardo [40] cuando se refieren a la relación que existe entre las Normas y modelos de riesgo de las tecnologías de información, donde se reconoce los elementos que las vincula aun cuando cada una puede detenerse en aspectos más detallados que sirven para robustecer las propuesta de articulación. En este caso la articulación permitió que el cumplimiento de la ley se diera se manera sistemática y ordenada, además tal como lo menciona De Freitas [26] la Norma ISO/IEC 270001 minimización los riesgos dentro del SGSI en la dinámica de la mejora continua.

Tras la identificación de los requerimientos de la Norma ISO/IEC 270001 y Ley a articular, la realización del diagnóstico acerca del nivel de cumplimiento permitió observar cómo se encontraba la institución universitaria en la intención de responder con

las disposiciones legales respecto de la Ley de protección de Datos personales y orientada bajo los lineamientos de calidad y gestión de riesgo que proporciona la Norma. Al respecto se pudo evidenciar que la Norma presenta un incumplimiento incipiente dentro de la institución. Cabe resaltar que, aunque su implementación no es obligatoria y la institución no se encuentra certificada este primer acercamiento a su uso permite un piloto sobre el cual se estaría evaluando la posibilidad de integrarla al sistema de calidad. Se espera, no obstante, que las directrices que proporciona se fortalezcan a partir del diseño y automatización del SGSI del Departamento de Sistemas de la institución, lo cual es necesario si se observa que el cumplimiento de la Ley, si bien tiene un porcentaje mayor (43%), aún no logra un cumplimiento completo como se exige. En otras palabras, dentro de procedimientos manuales la Ley ha avanzado, pero se espera que con el diseño y posterior consolidación del sistema de seguridad de información bajo la Norma ISO 27001 se logre un cumplimiento total de la protección de datos personales.

Frente a los riesgos evaluados, se observa que el DSI de la institución desconoce muchos (91%) de los controles de seguridad de la información que proporciona el Anexo A de la Norma ISO/IEC 27001, lo que indica que no han sido verificados en este contexto. Si bien existe una intención hacia la protección de la información y en cierta medida se logra no existe un proceso formal para realizar los controles, dejando los resultados a la suerte y al esfuerzo del personal calificado. Para ello, la automatización permitirá, como lo mencionan Martelo, Madera y Betín [41], el reconocimiento del estado de los documentos, gestión de la información para evitar la utilización de documentos que ya expiraron; la gestión de funciones y actividades; garantizar acceso, accesibilidad y seguimiento a documentos asignados. De esta manera, las operaciones de la institución

frente al cumplimiento no representarían una sobrecarga para el equipo de trabajo como lo menciona [17] y se estaría cumpliendo a las exigencias legales y a la Calidad.

El diseño y propiamente el proceso de automatización fueron posibles gracias a la identificación de requerimientos y al nivel de incumplimiento que reflejó el diagnóstico, estos permitieron el contexto de la investigación aplicada. La automatización siguió la estructura de organización que propone el software Eramba en su versión gratuita, la cual permite la seguridad de la información en la gestión del cumplimiento de las Normas y leyes, análisis y gestión de los riesgos y auditorías de los controles que gestionan los riesgos de la información en cualquier tipo de organización. Opción tecnológica que según Curtis [39] resulta beneficiosa para integrar el control y la seguridad las cuales representan ventajas si bien en los costos, también a nivel de la seguridad de la información, en tanto se haya analizado la pertinencia al adoptarlos.

Este aspecto en torno al uso del software libre resalta, además de la funcionalidad, el tema presupuestal, el cual puede presentarse como una limitación a la hora de migrar de un proceso manual de gestión de la seguridad de la información a un proceso automatizado, ya que el esfuerzo puede llegar a ser inútil si los costos superan el valor agregado que proporcione la herramienta de acuerdo con el panorama ofrecido por Advisera Expert Solution [29]. Sin embargo, al usar software libre se está posibilitando el cumplimiento de los objetivos, sin exceder el presupuesto de las organizaciones, por tanto, no se requiere necesariamente de sistemas sofisticados para la protección de datos a diferencia de los estiman Zhuo y Solak [38] y por lo cual proponen una alianza entre empresas para cubrir los altos costos.

Entre los aspectos evaluativos se destacaron las mejoras que proporcionó el SGSI orientado mediante la Norma ISO y la automatización, elemento agregado que aportó valor al ejercicio. En estos términos, la evaluación representa un factor con mucha influencia en la investigación y será el punto de partida para consolidar la herramienta dentro de la dinámica laboral, además, como menciona Ahman, Hendy y Abba [31], proporciona seguridad al sistema en la medida en que es posible identificar las fallas que luego serán subsanadas con las herramientas de control, lo que permite una herramienta más robusta para respaldar de manera incluso preventiva la seguridad de la información, atendiendo a la definición ofrecida por Godoy [45].

El cumplimiento de la norma de protección de los datos si bien es una exigencia para toda organización colombiana, la universidad no disponía de los mecanismos para responder con ella hasta que se presenta la oportunidad de diseñar un sistema basado en la Norma ISO 27001 que permite su gestión apoyada por la herramienta Eramba que finalmente logra su automatización logrando optimización en tal proceso. Durante el proceso se requirió el respaldo de quien representaría la Alta Gerencia para el caso, el Vicerrector Financiero quien tiene bajo su cargo las operaciones del DSI, elemento clave que referencian Valencia y Orozco [24] para el cumplimiento de los objetivos de un proyecto o investigación.

Capítulo VI. Conclusiones y Recomendaciones

6.1 Conclusiones

La identificación de los requerimientos que exige la Norma ISO 27001:2013 y la Ley 1581 sirvieron de contexto para analizar la totalidad de las exigencias que promueven el cumplimiento frente la protección de datos personales, la cual aplica para instituciones públicas y privadas a nivel nacional, en este sentido, también alerta sobre los riesgos administrativos y económicos que conllevaría para la institución universitaria el no cumplimiento.

Frente al cumplimiento, el diagnóstico puso de manifiesto los porcentajes de incumplimiento de la Ley y aún más del derrotero que propone la Norma para efecto de evitar los riesgos consecuencia del no cumplimiento, panorama que sustenta la necesidad de dar solución tecnológica a la problemática planteada. Por tanto, es necesario consolidar de manera simultánea los requerimientos de la Norma para avanzar hacia el cumplimiento completo de la Ley. Se reconoce, no obstante, que la institución

desde su Departamento de Sistemas de Información viene adelantando algunas acciones para la salvaguarda de la información y de los datos personales, sin embargo, la ausencia de un nivel de cumplimiento mayor se debe a que no había adelantado un proceso formal antes de la presente investigación, donde el diseño automatizado viene a proporcionar además de agilidad, eficacia, y eficiencia, una estructura formal a bajo costo que permita un cumplimiento completo de la Ley 1581. Lo que señala la potencialidad de abordar problemas organizacionales desde procesos de investigación.

Con respecto al diseño y automatización, se contó con una herramienta pertinente para gestionar adecuadamente los riesgos que podrían derivar del no cumplimiento. La pertinencia se valoró en términos de la seguridad de la información, la gestión del cumplimiento, transparencia a la hora de gestionar, almacenar y salvaguardar los datos y la posibilidad de lograr la escalabilidad de un proceso sin incurrir en costos adicionales.

De esta manera, se logró el diseño de un sistema automatizado de gestión de la seguridad de la información, sin embargo, la implantación y uso de la herramienta en las operaciones de la institución para efectos de gestión de la seguridad de la información podrán validad su carácter óptimo y ágil.

Por su parte, la evaluación del proceso de automatización permitió la identificación de las mejoras que la nueva herramienta proporciona al DSI en el interés por responder a la Ley de la protección de los datos, no obstante, se reconocen que tras la puesta en marcha del SGSI de manera formal en la institución surgirán nuevas oportunidades de mejora como la ya señalada en el documento frente al análisis de datos, la cual se puede resolver con la integración de otra herramienta de acceso abierto o de ser el caso, podría

integrarse la versión paga de Eramba que proporciona nuevas y mejores funcionalidades al proceso.

Por último, se menciona que el diseño del SGSI puede llevarse a cabo de diferentes formas y recursos, aquí se privilegió el logro de un objetivo a bajo costo, no obstante, el resultado fue posible gracias a la integración de una mirada sistémica que incluyó una ley, una norma y una plataforma de automatización.

6.2 Recomendaciones

Las recomendaciones se presentan a nivel técnico para garantizar, luego del diseño, la implantación del SGSI y a nivel del proceso investigativo de cara a generar nuevos avances aplicados en esta línea tanto para la misma institución universitaria, como para otro tipo de organización interesada en migrar a un sistema automatizado para la gestión de la seguridad de la información.

- Luego de implantado el SGSI se sugiere seguimiento interno y la auditoria anual por parte de una entidad externa a fin de que sirva de avaluación para los procesos internos. Esto contribuye también a la autoevaluación.
- Para el seguimiento interno se sugiere la construcción de una batería de indicadores de gestión.

- Se sugiere un ejercicio evaluativo luego de la implantación de SGSI a fin de reconocer las ventajas y desventajas que proporciona la automatización en estos procesos y qué tanto beneficio trae a las instituciones. De esta manera es posible evaluar con mayor profundidad las variables de agilidad y la optimización.
- El SGSI automatizado actualmente registra y analiza los riesgos ingresados por un humano para la toma de decisiones. Un nivel avanzado de las funciones de dicho sistema a modo de mejora considera enlazar el sistema a sensores que señalen cuándo se puede presentar un riesgo.
- El proceso de mejora tras la operación formal del SGSI en el DSI de la Universidad plantea la posible integración de herramientas complementarias para mejorar funciones en la misma línea del software de código abierto, siendo igualmente posible la integración de funciones pagas desde Eramba, lo que plantea una nueva fase que puede ser objeto de análisis en posteriores investigaciones en términos de evaluación de proceso como de resultados.

Referencias

[1] M. Monagas, «El capital intelectual y la gestión del conocimiento,» Ingeniería Industrial, vol. XXXIII, nº 2, pp. 142-150, 2012.

[2] O. J. Salcedo, C. A. Fernández y L. Castellanos, «Hackers en la sociedad de la información: análisis de su dinámica desde una perspectiva social,» Visión Electrónica, vol. 6, nº 1, pp. 115-125, Enero-Junio 2012.

[3] Congreso de la República de Colombia, Ley Estatutaria 1581 de 2012, Bogotá: Diario Oficial, 18.

[4] Superintendencia de Industria y Comercio, «Protección de Datos Personales,» 2020a. [En línea]. Available: https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales.

[5] Superintendencia de Industria y Comercio, «Registro Nacional de Bases de Datos,» 2020b. [En línea]. Available: https://www.sic.gov.co/registro-nacional-de-bases-de-datos.

[6] A. H. Velasco, «El derecho informático y la gestión de la eguridad de la información una pespectiva con base en la norma ISO 27001,» Rev. Derecho, pp. 333-336, 2008.

[7] Normas-ISO, «ISO 27001 Seguridad de la información,» 2020. [En línea]. Available: https://www.normas-iso.com/iso-27001/.

[8] Ministerio de Educación Nacional -MEN-. «Decreto 1330 de 2019,» Bogotá, 2019.

[9] A. Calder, ISO27001/ISO27002 Una guía de bolsillo, ITGP, 2017.

[10] M. I. Romero, G. L. Figueroa, D. S. Vera, J. E. Álava, G. Parrales, C. J. Álava, Á. L. Murillo y M. A. Castillo, Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades, Alcoy: Área de Innovación y Desarrollo, S.L., 2018.

[11] Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos, Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012.

[12] Ministerio de Comercio, Industria y Turismo, «Decreto Número 1377 de 2013 "Por el cual se reglamenta parcialmente la Ley 1581 de 2012",» Bogotá, 2013.

[13] Organización de los Estados Americanos -OEA-, «Estudio Comparativo:protección de datos en las Américas,» Comisión de Asuntos Jurídicos y Políticos, 2012.

[14] S. Ú. d. I. N. Suin-Juriscol-, «-Suin-Juriscol-,» 31 diciembre 2008. [En línea]. Available: http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1676616.

[15] DANE, «Diario oficial No. 41.083,» 20 octubre 1993. [En línea]. Available: https://www.dane.gov.co/files/sen/normatividad/Ley79_1993.pdf.

[16] Congreso de Colombia, «Ley Estatutaria 1581 de 2012,» 17 octubre 2012. [En línea]. Available: https://www.sisben.gov.co/Documents/Informaci%C3%B3n/Leyes/LEY%20TRATAMIENTO%20DE%20DATOS%20-%20LEY%201581%20DE%202012.pdf.

[17] D. Kosutic, «The ISO 27001 & ISO 22301,» 11 abril 2016. [En línea]. Available: https://advisera.com/27001academy/es/blog/.

[18] J. Lozada, «Investigación aplicada: definición, propiedad intelectual e industria,» Cienciamérica, nº 3, pp. 34-39, 2014.

[19] S. López, «Certificado ISO9001,» 9 abril 2018. [En línea]. Available: https://www.certificadoiso9001.com/que-es-iso/.

[20] I. L. O. ILO, «Database of national labour, social security and related human rights legislation» 29 01 2009. [En línea]. Available: https://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=80575&p_count=96738.

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

[22] L. Giraldo, «Análisis para la implementación de un sistema de gestión de seguridad de la información según la norma ISO 27001 en la empresa Servidoc S.A.,» Universidad Nacional Abierta y a distancia, Bogotá, 2016.

[23] R. Montesino, W. Baluja y J. Porvén, «Gestión automatizada e integrada de controles de seguridad informática,» RIELAC, nº 1, pp. 40-58, 2013.

[24] F. J. Valencia y M. Orozco, «Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000,» RISTI - Revista Iberica de Sistemas e Tecnologias de Información, nº 22, pp. 73-88, 2017.

[25] Marrugo Rivera, «La Seguridad de la Información en las Universidades en Colombia.,» 1 febrero 2018. [En línea]. Available:

https://marrugorivera.com/blog/2018/02/01/la-seguridad-de-la-informacion-en-las-universidades-en-colombia/.

[26] V. De Freitas, «Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar,» Enlace, 2009.

[27] F. Caviedes y B. A. Prado, Modelo unificado para identificación y valoración de los riesgos de los activos de información en una organización, Cali: Universidad ICESI, 2012, pp. 2-169.

[28] Advisera Express Solution, «How to Budget an ISO 27001 Implementation Project» pp. 1-13, 2016b.

[29] Advisera Express Solution, «Privacy cyber security and ISO 27001» Advisera, pp. 3-14, 2016a.

[30] Advisera Express Solution, «Implementing ISO 27001 with a consultant vs. DIY approach» Advisera, pp. 1-9, 2016c.

[31] F. Ahmad, C. Hendy y G. Abba, «Evaluation of ISO 27001 implementation towards information security of cloud service customer in PT. IndoDev Niaga Internet» Journal of Physics: Conference Series, nº 1, pp. 1-9, 2018.

[32] C. Cares y M. Diéguez, «Comparación de dos enfoques cuantitativos para seleccionar controles de seguridad de la información,» Revista Ibérica de Sistemas y Tecnología de Información, nº 38, pp. 113-128, 2019.

[33] P. Amogh y A. Jayshree, «Best practices of auditing in an organization using ISO 27001 standard» International Journal of Recent Technology and Engineering, nº 3, pp. 691-695, 2019.

[34] A. Ribagorda, «La protección de datos personales y la seguridad de la información,» Revista jurídica de Castilla y León, nº 16, pp. 373-400, 2008.

[35] S. Alcalde, A. Zeidler, C. Klein, C. F. Valdivielso y I. R. Marias, «Enabling personal privacy for pervasive computing environments» Journal of Universal Computer Science, vol. 16, nº 3, pp. 341-371, 2010.

[36] L. Galvis, «Protección de datos en Colombia, avances y retos,» Lebret, 2012.

[37] F. Pelloso, M. Aparecido, R. F. Frogeri y C. L. Leal, «A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos,» Suma de negocios, nº 23, pp. 89-99, 2019.

[38] Y. Zhuo y S. Solak, «Optimal Policies for Information Sharing in Information System Security» European Journal of Operational Research, pp. 1-50, 2019.

[39] I. Curtis, «Integrated Control and Safety» Measurement + Control, vol. 44, nº 5, pp. 145-149, 2011.

[40] A. Vanegas y C. Pardo, «Hacia un modelo para la gestión de riesgos de TI en MiPyMEs: MOGRIT,» Revista S&T, vol. 12, nº 30, pp. 35-48, 2014.

[41] R. J. Martelo, J. E. Madera y A. D. Betín, «Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI).,» Información tecnológica, vol. 26, nº 2, pp. 129-234, 2015.

[42] N. V. Syreyshchikova, D. Y. Pimenov, T. Mikolajczyk y L. Moldovan, «Information Safety Process Development According to ISO 27001 for an Industrial Enterprise» Procedia Manufacturing, pp. 278-285, 2019.

[43] A. Narain y M. Gupta, «Information Security Management» Global Business Review, vol. 20, nº 1, pp. 253-271, 2019.

[44] Á. J. Varela, L. Parody, R. Gasca y M. T. Gómez, «Automatic Verification and Diagnosis of Security Risk Assessments in Business Process Models» IEEE Access, vol. 7, pp. 264-265, 2019.

[45] R. Godoy, «Seguridad de la información,» de Seguridad de la información, Guatemala, Universidad de San Carlos de Guatemala, 2014, pp. 160-173.

[46] C. De Pablos, J. López, S. M. Romo y S. Medina, Organización y transformación de los sistemas de información en la empresa, Cuarta ed., Madrid: ESIC, 2019.

[47] J. F. Carpentier, La seguridad informática en la PYME, Barcelona: Ediciones ENI, 2016.

[48] R. Baldecchi, «Implementación efectiva de un SGSI ISO 27001,» 2014. [En línea]. Available: https://engage.isaca.org/communities/chapter.

[49] A. Garriga, Nuevos retos para la protección de datos personales. En la era del Big Data y de la computación ubicua, Madrid: Dykinson, 2016.

[50] J. Pérez, A. Agudín y A. García, La biblia del hacker, Madrid: Anaya, 2003.

[51] C. Ruedas, «Automatización industrial: áreas de aplicación para ingeniería,» Guatemala, 2008.

[52] R. Montesino, S. Fenz y W. Baluja, SIEM-based framework for security controls automation, Emerald Group Publishing Limited, 2012.

[53] Eramba, Eramba Community, C.2.8.1 ed., 2019.

[54] Instituto Nacional de Ciberseguridad, «Evaluación y análisis de riesgos,» 2020. [En línea]. Available: https://www.incibe.es/.

[55] C. Espinoza, Metodología de la investigación tecnológica Pensando en Sistemas, Sexta ed., Huancayo: Ciro Esponoza Montes, 2010.

[56] Mitsubishi Electric, «NC solutions,» El libro de la automatización, [En línea]. Available: https://www.ncsolutions.es/wp-content/uploads/2016/04/El-libro-de-la-automatizacion.pdf. [Último acceso: 26 febrero 2021].

[57] M. Menguzzato y J. J. Renau, La Dirección Estratégica de la empresa. Un enfoque innovador del Management, Barcelona: Ariel, 1991.

[58] R. Lapiedra, C. Devece y J. Guiral, Introducción a la gestión de sistemas de información en la empresa, Cataluña: Sapienta, 2011.

[59] J. Gómez, Optimización de Sistemas de Detección de Intrusos en Red Utilizando Técnicas Computacionales Avanzadas, Almería: Universidad de Almería, 2009.

[60] G. Westreicher, «La optimización,» Economipedia.com, 24 mayo 2020. [En línea]. Available: https://economipedia.com/definiciones/optimizacion.html.

[61] M. González, Gestión Eficaz del Tiempo, Málaga: Innovación y Cualificación S.L, 2006.

[62] M. Udaondo, Gestión de Calidad, Madrid: Ediciones Díaz de Santos S.A, 1992.

[63] J. R. Lozano, Cómo y dónde optimizar los costes logísticos: en el sistema integral de operaciones y en las diferentes áreas de actividad logística, Madrid: Fundación Confemetal, 2002.

[64] I. Guerra, Evaluación y mejorar continua. Conceptos y herramientas para la medición y mejorar del desempeño, Bloomington: AuthorHouse, 2007.

[65] M. Peñaloza, «Tecnlogía e Innovación factores claves para la competitividad,» Actualidad Contable Faces, vol. 10, nº 15, pp. 82-94, julio-diciembre 2007.

[66] J. Miguel, Protección de datos y seguridad de la información, 4 edición ed., Madrid: RA-MA, S.A, 2015.

[67] P. Aguilera, Seguridad informática, Editex, 2010.

[68] M. I. Jociles, «Laobservación participante: ¿consiste en hablar con "informantes"?,» Quaderns-e, vol. 1, nº 21, pp. 113-124, 2016.

[69] I. Pellicer, P. Vivas y J. Rojas, «La observación participante y la deriva: dos técnicas móviles para el análisis de la ciudad contemporánea,» EURE, vol. 39, nº 116, pp. 119-139, 2016.

[70] G. Campos y N. E. Lule, «La observación, un método para el estudio de la realidad,» Xihmai, vol. VII, nº 13, pp. 45-60, 2012.

[71] Universidad Autónoma del Estado de Hidalgo, «Catálogo de lista de cotejo,» [En línea]. Available: https://www.uaeh.edu.mx/division_academica/educacion-media/docs/2019/listas-de-cotejo.pdf. [Último acceso: 4 marzo 2021].

[72] D. C. Cheng y N. R. Lim-Cheng. «An ontology bases framework to support multi-standard compliance for an enterprise». Pp 1-6. 2017 DOI: 10.1109/ICRIIS.2017.8002514

[73] F. M. D. P. R. Chavez. «Hardening an Open-Source Governance Risk and Compliance Software: Eramba». Tesis de maestría, Universidad de Lisboa: 2020. Disponible: https://repositorio.ul.pt/bitstream/10451/48321/1/ulfc126374_tm_Miguel_Chaves.pdf

[74] M. Tenorio. «Caso de estudio del proceso de implementación de las Normas IEC/ISO 9001, IEC/ISO 27001 sobre un marco de referencia propuesto por Nist Fisma para la gestión de la seguridad de la información del producto de una empresa prestadora de servicios PAAS». Universidad Piloto de Colombia. 2014. Disponible: http://polux.unipiloto.edu.co:8080/00004651.pdf

Anexos

Anexo 1. *Principios para el tratamiento de datos personales*

Principios para el tratamiento de datos personales	
1	Se recolecta información personal para finalidades legítimas y se informa al Titular esas finalidades.
2	Se cuenta con el consentimiento previo, expreso e informado para el Tratamiento de datos de los Titulares de los cuales se recolecta información personal.
3	Si hay casos en los que se recolecta información personal sin el consentimiento de los Titulares, existe un mandato legal o judicial que habilite a la organización para hacerlo.
4	Se conserva información personal veraz, completa, exacta, actualizada, comprobable y comprensible.
5	Se cuenta con medidas técnicas para controlar y brindar un conocimiento restringido de la información personal solo a los Titulares o a terceros autorizados conforme a la ley.
6	Se cuenta con medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a la información personal para evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
7	Se garantiza la confidencialidad de la información por las personas de la organización que intervienen en el Tratamiento de datos personales, incluso después de que han finalizado su relación con alguna de las labores desempeñadas.
Tratamiento De Datos Sensibles Y De Menores De Edad	
8	Se cuenta con autorización explícita de los Titulares para el Tratamiento de sus datos sensibles.
9	Se Informa al Titular que por tratarse de datos sensibles no está obligado a autorizar su Tratamiento.
10	Se Informa al Titular cuáles de los datos que serán objeto de Tratamiento en su organización son sensibles y para qué finalidad(es) se utilizarán.
11	Se efectúa Tratamiento de datos personales de menores de edad únicamente para actividades que responden y respetan el interés superior de los menores.
12	En el Tratamiento de datos personales de menores de edad se asegura el respeto de sus derechos fundamentales.
13	Se cuenta con la autorización del representante legal del menor de edad para el tratamiento de sus datos.
Derechos de los titulares de información	

14	Se permite el ejercicio del derecho de los titulares a conocer, actualizar y rectificar los datos personales que recolecta.
15	Se da respuesta a las solicitudes presentadas por los Titulares es dentro de la oportunidad prevista en la ley general de protección de datos personales.
16	Se entrega a los Titulares copia de la autorización otorgada por ellos para el Tratamiento de sus datos personales cuando así lo solicitan estos.
17	Se informa a los Titulares qué uso les ha dado la organización a sus datos personales cuando así lo solicitan estos,
18	Se permite a los Titulares el acceso gratuito a los datos personales que han sido objeto de Tratamiento al menos una vez cada mes calendario y cada vez que se hagan modificaciones sustanciales a las Políticas de Tratamiento de la información.
Autorización para el tratamiento de datos personales	
19	Se cuenta con la autorización de los Titulares de los datos contenidos en las bases de datos que tiene la organización para el Tratamiento de los mismos.
20	Se conocen los casos en los que no es necesario contar con autorización de los Titulares para el Tratamiento de su información personal.
21	Se cuenta con procedimientos efectivos y eficientes para solicitar, a más tardar en el momento de la recolección de los datos personales, las autorizaciones de los Titulares para el Tratamiento de los mismos,
22	Se informa a los Titulares qué datos personales serán recolectados y todas las finalidades específicas del Tratamiento para las cuales la organización obtiene el consentimiento.
23	Se obtienen nuevas autorizaciones de los Titulares, cuando la organización realiza cambios sustanciales en las políticas de Tratamiento de información personal.
24	Se establecen mecanismos que garantizan la consulta posterior de la autorización otorgada por los Titulares para el Tratamiento de sus datos personales.
25	Se pone a disposición de los Titulares mecanismos gratuitos y de fácil acceso para presentar solicitudes de supresión de datos o la revocatoria de la autorización otorgada.
Información mínima a los titulares	
26	Se informa de manera clara y expresa a los Titulares, al momento de solicitar la autorización para el Tratamiento de datos personales, el Tratamiento al cual serán sometidos los mismos y la finalidad.
27	Se informa de manera clara y expresa a los Titulares, al momento de solicitar la autorización para el Tratamiento de datos personales, el carácter facultativo de la respuesta a las preguntas que se hacen,

	cuando se relacionan con datos sensibles o datos de niñas, niños y adolescentes.
28	Se informa de manera clara y expresa a los Titulares, al momento de solicitar la autorización para el Tratamiento de datos personales, los derechos que les asisten.
29	Se informa de manera clara y expresa a los Titulares, al momento de solicitar la autorización para el Tratamiento de datos personales, la identificación, dirección física y electrónica y teléfono del responsable del Tratamiento.
30	Se conserva prueba de haber informado a los Titulares lo mencionado anteriormente.
Suministro de la información personal	
31	La información personal que se suministra al Titular o a quien éste autorice es de fácil lectura, sin barreras técnicas que impidan su acceso y corresponde en un todo a aquella que reposa en la base de datos.
32	Se suministra únicamente información personal a los Titulares, sus causahabientes o Sus representantes legales, a las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial y a los terceros autorizados por el Titular o por la ley.
Atención de consultas y reclamos de los titulares	
33	Se cuenta con canales o mecanismos sencillos y ágiles y que estén permanentemente habilitados para la atención de las consultas y reclamos de los Titulares o sus causahabientes.
34	Se dan a conocer a los Titulares e interesados los canales habilitados para la atención de consultas y reclamos en la política de Tratamiento de datos personales dispuesta por la organización.
35	Se atiende, dentro de los diez (10) días hábiles contados a partir de su recibo, las consultas de información personal presentadas por los Titulares, sus causahabientes y las personas autorizadas.
36	Se informa a los peticionarios el motivo de la no atención oportuna a su consulta de información personal y se señala la fecha de respuesta de la solicitud, sin exceder el término de cinco (5) días adicionales a los diez (10) días iniciales para contestar.
37	Se atiende, dentro de los quince (15) días hábiles contados a partir de su recibo, las reclamaciones presentadas por los Titulares o sus causahabientes que consideran que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto Incumplimiento de cualquiera de los deberes contenidos en la ley.

38	38. Se informa a los peticionarios el motivo de la no atención oportuna a su reclamo y se señala la fecha de respuesta de la solicitud, sin exceder el término de ocho (8) días adicionales a los quince (15) días Iniciales para contestar.
39	39. Se adoptan medidas para asegurar que os datos personales que reposan en las bases de datos sean precisos y suficientes y, cuando así lo solicite el Titular o cuando haya podido advertirlo, sean actualizados, rectificados o suprimidos, de tal manera que satisfagan los propósitos del Tratamiento.
40	40. Se ha designado a una persona o área para que asuma la función de protección de datos personales y dé trámite a las solicitudes de los Titulares para el ejercicio de sus derechos.
Atención de consultas y reclamos de los titulares	
41	Se da a conocer a los Titulares los procedimientos dispuestos por la organización para el acceso, actualización, supresión y rectificación de datos personales y de revocatoria de la autorización, y los mismos son fácilmente accesibles.
42	Se incluye dentro de la política de Tratamiento de datos personales los procedimientos dispuestos para garantizar el acceso, actualización, supresión y rectificación de datos personales y de revocatoria de la autorización.
43	Se cuenta con un manual interno de políticas y procedimientos para garantizar la atención de consultas y reclamos presentados por los Titulares y para garantizar, en general, el adecuado cumplimiento de la ley.
44	Se han adoptado procesos para la atención y respuesta a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto del Tratamiento de sus datos personales.
Política de tratamiento de datos personales	
45	Se cuenta con una política para el Tratamiento de los datos personales.
46	La política para el Tratamiento de datos personales consta en medio físico o electrónico, en un lenguaje claro y sencillo, y es puesta en conocimiento de los Titulares.
47	Se cuenta con una política para el Tratamiento de datos personales que incluye el nombre o razón social, domicilio, dirección, correo electrónico y teléfono de la organización.
48	La política para el tratamiento de datos adoptada por la organización incluye información sobre el Tratamiento al cual serán sometidos los datos personales y a finalidad del mismo.
49	Incluye la política para el tratamiento de datos personales información sobre los derechos que le asisten a los Titulares respecto de su información personal.

50	Se informa en la política para el Tratamiento de datos personales sobre la persona o área Responsable de la atención de peticiones, consultas y reclamos ante la cual el Titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.
51	Se indica en la política para el Tratamiento de datos personales cuál o cuáles son los procedimientos para que los Titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización.
52	En la política para el Tratamiento de datos personales está Incluida la fecha de entrada en vigor y el período de vigencia de la o las bases de datos que tiene la organización.
Aviso de privacidad	
53	Se informa a los Titulares la existencia de políticas para el tratamiento de datos personales por medio de un aviso de privacidad.
54	El aviso de privacidad publicado por la organización incluye el nombre o razón social y los datos de contacto de esta.
55	En el aviso de privacidad publicado se incluye la descripción del tratamiento al cual serán sometidos los datos personales recolectados y la finalidad de tal recolección.
56	El aviso de privacidad incluye un listado de los derechos que tienen los Titulares cuya información es recolectada por la organización.
57	Se informa a los Titulares en el aviso de privacidad publicado, cómo acceder o consultar la política de Tratamiento de datos personales dispuesta por la organización.
58	En el aviso de privacidad publicado se señala expresamente la facultad que tienen los Titulares de contestar o no las preguntas que versen sobre datos personales sensibles o sobre los datos de niños, niñas y adolescentes.
59	Se conserva el modelo de aviso de privacidad utilizado para cumplir con la obligación legal de dar a conocer las políticas de Tratamiento de la información personal.
Reporte de violaciones a los códigos de seguridad	
60	Informa a la Superintendencia cuando se presentan violaciones a los códigos de seguridad que generen riesgos en la administración de la información de los Titulares.
Gestión de encargados del tratamiento	
61	Se han establecido procedimientos internos para asegurar que los encargados del Tratamiento garanticen la protección de los datos personales que le son entregados y que su Tratamiento se haga acorde con los principios y deberes establecidos en la ley.

62	Se suscriben contratos con los encargados que incluyan expresamente el tratamiento que éste podrá realizar a los datos personales.
63	Se suscriben contratos con los Encargados que incluyan cláusulas de confidencialidad de la Información entregada.
64	Se exige a los Encargados tener y mantener políticas de seguridad de la información y de Tratamiento de datos personales antes de entregar las bases de datos.
65	Se Informa al Encargado de forma oportuna todas las novedades respecto de los datos que previamente le fueron suministradas.
66	Se cuenta con medidas necesarias para que la información suministrada al Encargado se mantenga actualizada.
67	Se comunica al Encargado cuando se ha rectificado la información Incorrecta
68	Se comunica al Encargado si determinada información se encuentra en discusión por parte del Titular, una vez éste presenta una reclamación y no ha finalizado el trámite respectivo.
69	Se verifica que el Encargado actualice y rectifique la información personal en los términos legales.
Transferencia y transmisión internacional de datos personales	
70	Se transfieren datos personales a países que garantizan niveles adecuados de protección de datos, según lo establecido en el numeral del Capítulo Tercero del Título V de la Circular Única de la Superintendencia de industria y comercio.
71	Se han implementado medidas apropiadas y efectivas para garantizar el adecuado Tratamiento de los datos personales que se transfieren a otro país y para otorgar seguridad a los registros al momento de efectuar dicha transferencia.
72	Se transfieren datos personales fuera del territorio colombiano con base en alguna de las causales de excepción establecidas en el artículo 26 de la Ley 1581 de
73	Se transfieren datos personales fuera del territorio colombiano con base en una declaración de conformidad emitida por esta Superintendencia.
74	Se han suscrito contratos con los Responsables del Tratamiento destinatarios de los datos personales a transferir fuera del territorio colombiano o se implementan otros instrumentos jurídicos en los que señalen las condiciones que regirán la transferencia internacional de datos personales, mediante las cuales se garantizará el cumplimiento de los principios que rigen el Tratamiento, así como de las obligaciones que tienen a cargo.

75	Se transmiten datos personales fuera del territorio colombiano a un encargado para que realice el Tratamiento indicado por la organización como Responsable del Tratamiento y para ello se han suscrito contratos de transmisión de datos personales en los que se señalen los alcances del Tratamiento, las actividades que el encargado realizará y las obligaciones de este respecto de los Titulares y el Responsable.
76	Se incluyen en el contrato de transmisión internacional de datos personales celebrado con el Encargado cláusulas mediante las cuales este se compromete a dar aplicación a las obligaciones del Responsable bajo Su política de Tratamiento de la información y a realizar el Tratamiento de datos de acuerdo con la finalidad que los Titulares han autorizado y con las leyes aplicables.
77	Se incluye en el contrato de transmisión internacional de datos personales celebrado con el Encargado la obligación de dar Tratamiento, a nombre del Responsable, a los datos personales conforme a los principios establecidos en la ley general de protección de datos personales.
78	Se incluye en el contrato de transmisión internacional de datos personales celebrado con el Encargado la obligación para este de salvaguardar la seguridad de las bases de datos que contengan datos personales.
79	Se incluye en el contrato de transmisión internacional de datos personales celebrado con el Encargado la obligación para este de guardar confidencialidad respecto del Tratamiento de los datos personales.
Responsabilidad demostrada	
80	Se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y el Decreto Único 1074 de 2015 de manera proporcional a la naturaleza jurídica de la organización y su tamaño empresarial.
81	Se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y el Decreto único 1074 de 2015 de manera proporcional a la naturaleza de los datos personales Objeto del Tratamiento.
82	Se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y el Decreto Único 1074 de 2015 de manera proporcional al tipo de Tratamiento que realice con los datos personales.
83	Se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y el Decreto Único 1074 de 2015 de manera proporcional a los riesgos potenciales que el Tratamiento podría causar sobre los derechos de los Titulares.

84	Se conserva evidencia sobre la implementación efectiva de medidas de seguridad apropiadas para el cumplimiento del régimen de protección de datos personales.
85	Se han adoptado mecanismos internos para poner en práctica las políticas establecidas en los que se incluyan herramientas de implementación, entrenamiento y programas de educación en materia de protección de datos personales.
Registro nacional de bases de datos	
86	86. Se han registrado las bases de datos con información personal de la organización en el Registro Nacional de Bases de Datos (RNBD), administrado por la Superintendencia de Industria y Comercio

Anexo 2. *Nivel de cumplimiento a los requisitos de la Norma ISO 27001.*

Nivel de cumplimiento a los requisitos de la Norma ISO 27001 DSI		
Sección	**Requerimientos ISO 27001**	**Nivel**
4	**Contexto de la organización**	
4,1	**Comprensión de la organización y de su contexto**	
4,1	Determinar los objetivos del SGSI de la organización y cualquier problema que pueda afectar su eficacia	Inicial
4,2	**Comprensión de las necesidades y expectativas de las partes interesadas**	
4.2 (a)	Identificar las partes interesadas incluyendo leyes aplicables, regulaciones, contratos, etc.	Definido
4.2 (b)	Determinar los requerimientos y obligaciones relevantes de seguridad de la información	Inicial
4,3	**Determinación del alcance del SGSI**	

4,3	Determinar y documentar el alcance del SGSI	Inicial
4,4	**SGSI**	
4,4	Establecer, implementar, mantener y mejorar de forma continua el SGSI acorde al estándar	Inexistente
5	**Liderazgo**	
5,1	**Liderazgo y compromiso**	
5,1	La administración debe demostrar liderazgo y compromiso por el SGSI	Inexistente
5,2	**Política**	
5,2	Documentar la Política de Seguridad de la Información	Inicial
5,3	**Roles, responsabilidades y autoridades en la organización**	
5,3	Asignar y comunicar los roles y responsabilidades de seguridad de la información	Inicial
6	**Planificación**	
6,1	**Acciones para tratar los riesgos y oportunidades**	
6.1.1	Diseñar el SGSI para satisfacer los requerimientos, tratando riesgos e identificando oportunidades	Inexistente
6.1.2	Definir e implementar un proceso de análisis de riesgos de seguridad de la información	Inexistente
6.1.3	Documentar e implementar un proceso de tratamiento de riesgos de seguridad de la información	Inexistente
6,2	**Objetivos de seguridad de la información y planificación para su consecución**	

6,2	Establecer y documentar los planes y objetivos de la seguridad de la información	Inexistente
7	**Soporte**	
7,1	**Recursos**	
7,1	Determinar y asignar los recursos necesarios para el SGSI	Administrado
7,2	**Competencia**	
7,2	Determinar, documentar hacer disponibles las competencias necesarias	Inicial
7,3	**Concienciación**	
7,3	Implementar un programa de concienciación de seguridad	Inexistente
7,4	**Comunicación**	
7,4	Determinar la necesidades de comunicación internas y externas relacionadas al SGSI	Inexistente
7,5	**Información documentada**	
7.5.1	Proveer documentación requerida por el estándar más la requerida por la organización	Inexistente
7.5.2	Proveer un título, autor, formato consistente, revisión y aprobación a los documentos	Inicial
7.5.3	Mantener un control adecuado de la documentación	Definido
8	**Operación**	
8,1	**Planificación y control operacional**	
8,1	Planificar, implementar, controlar y documentar el proceso de gestión de	Inexistente

	riesgos del SGSI (Tratamiento de riesgos)	
8,2	**Apreciación de los riesgos de seguridad de la información**	
8,2	Evaluar y documentar los riesgos de seguridad regularmente y cuando hay cambios	Inexistente
8,3	**Tratamiento de los riesgos de seguridad de la información**	
8,3	Implementar un plan de tratamiento de riesgos y documentar los resultados	Inexistente
9	**Evaluación del desempeño**	
9,1	**Seguimiento, medición, análisis y evaluación**	
9,1	Realizar un seguimiento, medición, análisis y evaluación del SGSI y los controles	Inexistente
9,2	**Auditoría interna**	
9,2	Planificar y realizar una auditoría interna del SGSI	Inexistente
9,3	**Revisión por la dirección**	
9,3	La administración realiza una revisión periódica del SGSI	Inexistente
10	**Mejora**	
10,1	**No conformidad y acciones correctivas**	
10,1	Identificar, arreglar y reaccionar ante no conformidades para evitar su recurrencia documentando todas las acciones	Inexistente
10,2	**Mejora continua**	
10,2	Mejora continua del SGSI	Inexistente

Anexo 3. *Cumplimiento de los principios y deberes*

LISTADO DE COMPROBACIÓN RÉGIMEN DE PROTECCION DE DATOS PERSONALES - VERIFICAR EL CUMPLIMIENTO DE LOS PRINCIPIOS Y DEBERES ESTABLECIDOS EN LA LEY 1581 DE 2012	CUMPLIMIENTO
PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES	
1. Se recolecta información personal para finalidades legítimas y se informa al Titular esas finalidades.	SI CUMPLE
2. Se cuenta con el consentimiento previo, expreso e informado para el Tratamiento de datos de los Titulares de los cuales se recolecta información personal.	NO CUMPLE
3. Si hay casos en los que se recolecta información personal sin el consentimiento de los Titulares, existe un mandato legal o judicial que habilite a la organización para hacerlo.	NO CUMPLE
4. Se conserva información personal veraz, completa, exacta, actualizada, comprobable y comprensible.	SI CUMPLE
5. Se cuenta con medidas técnicas para controlar y brindar un conocimiento restringido de la información personal solo a los Titulares o a terceros autorizados conforme a la ley.	SI CUMPLE
6. Se cuenta con medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a la información personal para evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.	SI CUMPLE
7. Se garantiza la confidencialidad de la información por las personas de la organización que intervienen en el Tratamiento de datos personales, incluso después de que han finalizado su relación con alguna de las labores desempeñadas.	NO CUMPLE

TRATAMIENTO DE DATOS SENSIBLES Y DE MENORES DE EDAD	
8. Se cuenta con autorización explícita de los Titulares para el Tratamiento de sus datos sensibles.	NO CUMPLE
9. Se Informa al Titular que por tratarse de datos sensibles no está obligado a autorizar su Tratamiento.	NO CUMPLE
10. Se Informa al Titular cuáles de los datos que serán objeto de Tratamiento en su organización son sensibles y para qué finalidad(es) se utilizarán.	NO CUMPLE
11. Se efectúa Tratamiento de datos personales de menores de edad únicamente para actividades que responden y respetan el interés superior de los menores.	SI CUMPLE
12. En el Tratamiento de datos personales de menores de edad se asegura el respeto de sus derechos fundamentales.	SI CUMPLE
13. Se cuenta con la autorización del representante legal del menor de edad para el tratamiento de sus datos.	NO CUMPLE
DERECHOS DE LOS TITULARES DE INFORMACION	
14. Se permite el ejercicio del derecho de los Titulares a conocer, actualizar y rectificar los datos personales que recolecta.	SI CUMPLE
15. Se da respuesta a las solicitudes presentadas por los Titulares es dentro de la oportunidad prevista en la ley general de protección de datos personales.	SI CUMPLE
16. Se entrega a los Titulares copia de la autorización otorgada por ellos para el Tratamiento de sus datos personales cuando así lo solicitan estos.	NO CUMPLE
17. Se informa a los Titulares qué uso les ha dado la organización a sus datos personales cuando así lo solicitan estos,	SI CUMPLE
18. Se permite a los Titulares el acceso gratuito a los datos personales que han sido objeto de Tratamiento al menos una vez cada mes calendario y cada vez que se hagan modificaciones sustanciales a las Políticas de Tratamiento de la información.	SI CUMPLE

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES	
19. Se cuenta con la autorización de los Titulares de los datos contenidos en las bases de datos que tiene la organización para el Tratamiento de los mismos.	SI CUMPLE
20. Se conocen los casos en los que no es necesario contar con autorización de los Titulares para el Tratamiento de su información personal.	NO CUMPLE
21. Se cuenta con procedimientos efectivos y eficientes para solicitar, a más tardar en el momento de la recolección de los datos personales, las autorizaciones de los Titulares para el Tratamiento de los mismos,	SI CUMPLE
22. Se informa a los Titulares qué datos personales serán recolectados y todas las finalidades específicas del Tratamiento para las cuales la organización obtiene el consentimiento.	NO CUMPLE
23. Se obtienen nuevas autorizaciones de los Titulares, cuando la organización realiza cambios sustanciales en las políticas de Tratamiento de información personal.	NO CUMPLE
24. Se establecen mecanismos que garantizan la consulta posterior de la autorización otorgada por los Titulares para el Tratamiento de sus datos personales.	NO CUMPLE
25. Se pone a disposición de los Titulares mecanismos gratuitos y de fácil acceso para presentar solicitudes de supresión de datos o la revocatoria de la autorización otorgada.	NO CUMPLE
INFORMACION MÍNIMA A LOS TITULARES	
26. Se informa de manera clara y expresa a los Titulares, al momento de solicitar la autorización para el Tratamiento de datos personales, el Tratamiento al cual serán sometidos los mismos y la finalidad.	SI CUMPLE
27. Se informa de manera clara y expresa a los Titulares, al momento de solicitar la autorización para el Tratamiento de datos personales, el carácter facultativo de la respuesta a las	SI CUMPLE

preguntas que se hacen, cuando se relacionan con datos sensibles o datos de niñas, niños y adolescentes.	
28. Se informa de manera clara y expresa a los Titulares, al momento de solicitar la autorización para el Tratamiento de datos personales, los derechos que les asisten.	SI CUMPLE
29. Se informa de manera clara y expresa a los Titulares, al momento de solicitar la autorización para el Tratamiento de datos personales, la identificación, dirección física y electrónica y teléfono del Responsable del Tratamiento.	SI CUMPLE
30. Se conserva prueba de haber informado a los Titulares lo mencionado anteriormente.	SI CUMPLE
SUMINISTRO DE LA INFORMACION PERSONAL	
31. La información personal que se suministra al Titular o a quien éste autorice es de fácil lectura, sin barreras técnicas que impidan su acceso y corresponde en un todo a aquella que reposa en la base de datos.	SI CUMPLE
32. Se suministra únicamente información personal a los Titulares, sus causahabientes o Sus representantes legales, a las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial y a los terceros autorizados por el Titular o por la ley.	SI CUMPLE
ATENCION DE CONSULTAS Y RECLAMOS DE LOS TITULARES	
33. Se cuenta con canales o mecanismos sencillos y ágiles y que estén permanentemente habilitados para la atención de las consultas y reclamos de los Titulares o sus causahabientes.	SI CUMPLE
34. Se dan a conocer a los Titulares e interesados los canales habilitados para la atención de consultas y reclamos en la política de Tratamiento de datos personales dispuesta por la organización,	SI CUMPLE
35. Se atiende, dentro de los diez (10) días hábiles contados a partir de su recibo, las consultas de información	SI CUMPLE

personal presentadas por los Titulares, sus causahabientes y las personas autorizadas.	
36. Se informa a los peticionarios el motivo de la no atención oportuna a su consulta de información personal y se señala la fecha de respuesta de la solicitud, sin exceder el término de cinco (5) días adicionales a los diez (10) días iniciales para contestar.	SI CUMPLE
37. Se atiende, dentro de los quince (15) días hábiles contados a partir de su recibo, las reclamaciones presentadas por los Titulares o sus causahabientes que consideran que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto Incumplimiento de cualquiera de los deberes contenidos en la ley.	SI CUMPLE
38. Se informa a los peticionarios el motivo de la no atención oportuna a su reclamo y se señala la fecha de respuesta de la solicitud, sin exceder el término de ocho (8) días adicionales a los quince (15) días Iniciales para contestar.	SI CUMPLE
39. Se adoptan medidas para asegurar que os datos personales que reposan en las bases de datos sean precisos y suficientes y, cuando así lo solicite el Titular o cuando haya podido advertirlo, sean actualizados, rectificados o suprimidos, de tal manera que satisfagan los propósitos del Tratamiento.	SI CUMPLE
40. Se ha designado a una persona o área para que asuma la función de protección de datos personales y dé trámite a las solicitudes de los Titulares para el ejercicio de sus derechos.	SI CUMPLE
ATENCION DE CONSULTAS Y RECLAMOS DE LOS TITULARES	
41. Se da a conocer a los Titulares los procedimientos dispuestos por la organización para el acceso, actualización, supresión y rectificación de datos personales y de revocatoria de la autorización, y los mismos son fácilmente accesibles.	NO CUMPLE
42. Se incluye dentro de la política de Tratamiento de datos personales los procedimientos dispuestos para garantizar el	NO CUMPLE

acceso, actualización, supresión y rectificación de datos personales y de revocatoria de la autorización.	
43. Se cuenta con un manual interno de políticas y procedimientos para garantizar la atención de consultas y reclamos presentados por los Titulares y para garantizar, en general, el adecuado cumplimiento de la ley.	NO CUMPLE
44. Se han adoptado procesos para la atención y respuesta a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto del Tratamiento de sus datos personales.	NO CUMPLE
POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES	
45. Se cuenta con una política para el Tratamiento de los datos personales.	SI CUMPLE
46. La política para el Tratamiento de datos personales consta en medio físico o electrónico, en un lenguaje claro y sencillo, y es puesta en conocimiento de los Titulares.	SI CUMPLE
47. Se cuenta con una política para el Tratamiento de datos personales que incluye el nombre o razón social, domicilio, dirección, correo electrónico y teléfono de la organización.	SI CUMPLE
48. La política para el tratamiento de datos adoptada por la organización incluye información sobre el Tratamiento al cual serán sometidos los datos personales y a finalidad del mismo. I	SI CUMPLE
49. Incluye la política para el tratamiento de datos personales información sobre los derechos que le asisten a los Titulares respecto de su información personal.	SI CUMPLE
50. Se informa en la política para el Tratamiento de datos personales sobre la persona o área Responsable de la atención de peticiones, consultas y reclamos ante la cual el Titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.	SI CUMPLE
51. Se indica en la política para el Tratamiento de datos personales cuál o cuáles son los procedimientos para que los Titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización.	SI CUMPLE

52. En la política para el Tratamiento de datos personales está Incluida la fecha de entrada en vigencia y el período de vigencia de la o las bases de datos que tiene la organización.	SI CUMPLE
AVISO DE PRIVACIDAD	
53. Se informa a los Titulares la existencia de políticas para el tratamiento de datos personales por medio de un aviso de privacidad.	NO CUMPLE
54. El aviso de privacidad publicado por la organización incluye el nombre o razón social y los datos de contacto de la misma.	NO CUMPLE
55. En el aviso de privacidad publicado se incluye la descripción del tratamiento al cual serán sometidos los datos personales recolectados y la finalidad de tal recolección.	NO CUMPLE
56. El aviso de privacidad incluye un listado de los derechos que tienen los Titulares cuya información es recolectada por la organización.	NO CUMPLE
57. Se informa a los Titulares en el aviso de privacidad publicado, cómo acceder o consultar la política de Tratamiento de datos personales dispuesta por la organización.	NO CUMPLE
58. En el aviso de privacidad publicado se señala expresamente la facultad que tienen los Titulares de contestar o no las preguntas que versen sobre datos personales sensibles o sobre los datos de niños, niñas y adolescentes.	NO CUMPLE
59. Se conserva el modelo de aviso de privacidad utilizado para cumplir con la obligación legal de dar a conocer las políticas de Tratamiento de la información personal.	NO CUMPLE
REPORTE DE VIOLACIONES A LOS CÓDIGOS DE SEGURIDAD	
60. Informa a la Superintendencia cuando se presentan violaciones a los códigos de seguridad que generen riesgos en la administración de la información de los Titulares.	NO CUMPLE

GESTIÓN DE ENCARGADOS DEL TRATAMIENTO	
61. Se han establecido procedimientos internos para asegurar que los encargados del Tratamiento garanticen la protección de los datos personales que le son entregados y que su Tratamiento se haga acorde con los principios y deberes establecidos en la ley.	NO CUMPLE
62. Se suscriben contratos con los encargados que incluyan expresamente el tratamiento que éste podrá realizar a los datos personales.	NO CUMPLE
63. Se suscriben contratos con los Encargados que incluyan cláusulas de confidencialidad de la Información entregada.	NO CUMPLE
64. Se exige a los Encargados tener y mantener políticas de seguridad de la información y de Tratamiento de datos personales antes de entregar las bases de datos.	NO CUMPLE
65. Se Informa al Encargado de forma oportuna todas las novedades respecto de los datos que previamente le fueron suministradas.	NO CUMPLE
66. Se cuenta con medidas necesarias para que la información suministrada al Encargado se mantenga actualizada.	SI CUMPLE
67. Se comunica al Encargado cuando se ha rectificado la información Incorrecta	NO CUMPLE
68. Se comunica al Encargado si determinada información se encuentra en discusión por parte del Titular, una vez éste presenta una reclamación y no ha finalizado el trámite respectivo.	NO CUMPLE
69. Se verifica que el Encargado actualice y rectifique la información personal en los términos legales.	NO CUMPLE
TRANSFERENCIA Y TRANSMISIÓN INTERNACIONAL DE DATOS PERSONALES	
70. Se transfieren datos personales a países que garantizan niveles adecuados de protección de datos, según lo establecido en el numeral del Capítulo Tercero del Título V	NO CUMPLE

de la Circular Única de la Superintendencia de industria y comercio.	
71. Se han implementado medidas apropiadas y efectivas para garantizar el adecuado Tratamiento de los datos personales que se transfieren a otro país y para otorgar seguridad a los registros al momento de efectuar dicha transferencia.	NO CUMPLE
72. Se transfieren datos personales fuera del territorio colombiano con base en alguna de las causales de excepción establecidas en el artículo 26 de la Ley 1581 de	NO CUMPLE
73. Se transfieren datos personales fuera del territorio colombiano con base en una declaración de conformidad emitida por esta Superintendencia.	NO CUMPLE
74. Se han suscrito contratos con los Responsables del Tratamiento destinatarios de los datos personales a transferir fuera del territorio colombiano o se implementan otros instrumentos jurídicos en los que señalen las condiciones que regirán la transferencia internacional de datos personales, mediante las cuales se garantizará el cumplimiento de los principios que rigen el Tratamiento, así como de las obligaciones que tienen a cargo.	NO CUMPLE
75. Se transmiten datos personales fuera del territorio colombiano a un encargado para que realice el Tratamiento indicado por la organización como Responsable del Tratamiento y para ello se han suscrito contratos de transmisión de datos personales en los que se señalen los alcances del Tratamiento, las actividades que el encargado realizará y las obligaciones de este respecto de los Titulares y el Responsable.	NO CUMPLE
76. Se incluyen en el contrato de transmisión internacional de datos personales celebrado con el Encargado cláusulas mediante las cuales este se compromete a dar aplicación a las obligaciones del Responsable bajo Su política de Tratamiento de la información y a realizar el Tratamiento de datos de acuerdo con la finalidad que los Titulares han autorizado y con las leyes aplicables.	NO CUMPLE
77. Se incluye en el contrato de transmisión internacional de datos personales celebrado con el Encargado la obligación de dar Tratamiento, a nombre del Responsable, a los datos personales conforme a los principios establecidos en la ley general de protección de datos personales.	NO CUMPLE

78. Se incluye en el contrato de transmisión internacional de datos personales celebrado con el Encargado la obligación para este de salvaguardar la seguridad de las bases de datos que contengan datos personales.	NO CUMPLE
79. Se incluye en el contrato de transmisión internacional de datos personales celebrado con el Encargado la obligación para este de guardar confidencialidad respecto del Tratamiento de los datos personales.	NO CUMPLE
RESPONSABILIDAD DEMOSTRADA	
80. Se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y el Decreto Único 1074 de 2015 de manera proporcional a la naturaleza jurídica de la organización y su tamaño empresarial.	NO CUMPLE
81. Se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y el Decreto único 1074 de 2015 de manera proporcional a la naturaleza de los datos personales Objeto del Tratamiento.	NO CUMPLE
82. Se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y el Decreto Único 1074 de 2015 de manera proporcional al tipo de Tratamiento que realice con los datos personales.	NO CUMPLE
83. Se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y el Decreto Único 1074 de 2015 de manera proporcional a los riesgos potenciales que el Tratamiento podría causar sobre los derechos de los Titulares.	NO CUMPLE
84. Se conserva evidencia sobre la implementación efectiva de medidas de seguridad apropiadas para el cumplimiento del régimen de protección de datos personales.	NO CUMPLE
85. Se han adoptado mecanismos internos para poner en práctica las políticas establecidas en los que se incluyan herramientas de implementación, entrenamiento y programas de educación en materia de protección de datos personales.	NO CUMPLE

REGISTRO NACIONAL DE BASES DE DATOS	
86. Se han registrado las bases de datos con información personal de la organización en el Registro Nacional de Bases de Datos (RNBD), administrado por la Superintendencia de Industria y Comercio	SI CUMPLE
	86

Anexo 4. Listado de comprobación y cumplimiento régimen de protección de datos personales según ISO 27001/2013

	LEY 1581 - LISTADO DE COMPROBACIÓN y CUMPLIMIENTO RÉGIMEN DE PROTECCION DE DATOS PERSONALES				
	LISTADO	**¿Se encuentra en ISO?**	**ISO 27001**	**CONTROL**	**NOMBRE DEL CONTROL**
1	**PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES**				
1	Se recolecta información personal para finalidades legítimas y se informa al Titular esas finalidades.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
2	Se cuenta con el consentimiento previo, expreso e informado para el Tratamiento de datos de los Titulares de los cuales se recolecta información personal.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
3	Si hay casos en los que se recolecta información personal sin el consentimiento de los Titulares, existe un mandato legal o judicial que habilite a la organización para hacerlo.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
4	Se conserva información personal veraz, completa, exacta, actualizada, comprobable y comprensible.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
5	Se cuenta con medidas técnicas para controlar y brindar un conocimiento restringido de la información personal solo a los Titulares o a terceros autorizados conforme a la ley.	SI ISO 27001	8.1	A12.1.1	Documentación de procedimientos operacionales
6	Se cuenta con medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a la información personal para	SI ISO 27001	8.1	A12.1.1	Documentación de procedimientos operacionales

	evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.				
7	Se garantiza la confidencialidad de la información por las personas de la organización que intervienen en el Tratamiento de datos personales, incluso después de que han finalizado su relación con alguna de las labores desempeñadas.	SI ISO 27001	7.3	A7.2.1	Responsabilidades de gestión
2	**TRATAMIENTO DE DATOS SENSIBLES Y DE MENORES DE EDAD**				
8	Se cuenta con autorización explícita de los Titulares para el Tratamiento de sus datos sensibles.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
9	Se Informa al Titular que por tratarse de datos sensibles no está obligado a autorizar su Tratamiento.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
10	Se Informa al Titular cuáles de los datos que serán objeto de Tratamiento en su organización son sensibles y para qué finalidad(es) se utilizarán.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
11	Se efectúa Tratamiento de datos personales de menores de edad únicamente para actividades que responden y respetan el interés superior de los menores.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
12	En el Tratamiento de datos personales de menores de edad se asegura el respeto de sus derechos fundamentales.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
13	Se cuenta con la autorización del representante legal del menor de edad para el tratamiento de sus datos.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
3	**DERECHOS DE LOS TITULARES DE INFORMACION**				

14	Se permite el ejercicio del derecho de los Titulares a conocer, actualizar y rectificar los datos personales que recolecta.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
15	Se da respuesta a las solicitudes presentadas por los Titulares es dentro de la oportunidad prevista en la ley general de protección de datos personales.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
16	Se entrega a los Titulares copia de la autorización otorgada por ellos para el Tratamiento de sus datos personales cuando así lo solicitan estos.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
17	Se informa a los Titulares qué uso les ha dado la organización a sus datos personales cuando así lo solicitan estos,	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
18	Se permite a los Titulares el acceso gratuito a los datos personales que han sido objeto de Tratamiento al menos una vez cada mes calendario y cada vez que se hagan modificaciones sustanciales a las Políticas de Tratamiento de la información.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
4	**AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES**				
19	Se cuenta con la autorización de los Titulares de los datos contenidos en las bases de datos que tiene la organización para el Tratamiento de los mismos.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
20	Se conocen los casos en los que no es necesario contar con autorización de los Titulares para el Tratamiento de su información personal.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales

21	Se cuenta con procedimientos efectivos y eficientes para solicitar, a más tardar en el momento de la recolección de los datos personales, las autorizaciones de los Titulares para el Tratamiento de los mismos,	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
22	Se informa a los Titulares qué datos personales serán recolectados y todas las finalidades específicas del Tratamiento para las cuales la organización obtiene el consentimiento.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
23	Se obtienen nuevas autorizaciones de los Titulares, cuando la organización realiza cambios sustanciales en las políticas de Tratamiento de información personal.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
24	Se establecen mecanismos que garantizan la consulta posterior de la autorización otorgada por los Titulares para el Tratamiento de sus datos personales.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
25	Se pone a disposición de los Titulares mecanismos gratuitos y de fácil acceso para presentar solicitudes de supresión de datos o la revocatoria de la autorización otorgada.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
5	**INFORMACION MÍNIMA A LOS TITULARES**				
26	Se informa de manera clara y expresa a los Titulares, al momento de solicitar la autorización para el Tratamiento de datos personales, el Tratamiento al cual serán sometidos los mismos y la finalidad.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
27	Se informa de manera clara y expresa a los Titulares, al momento de solicitar la autorización para el Tratamiento de datos personales, el carácter facultativo de la respuesta a las preguntas que se hacen, cuando se relacionan con datos sensibles o datos de niñas, niños y adolescentes.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales

28	Se informa de manera clara y expresa a los Titulares, al momento de solicitar la autorización para el Tratamiento de datos personales, los derechos que les asisten.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
29	Se informa de manera clara y expresa a los Titulares, al momento de solicitar la autorización para el Tratamiento de datos personales, la identificación, dirección física y electrónica y teléfono del Responsable del Tratamiento.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
30	Se conserva prueba de haber informado a los Titulares lo mencionado anteriormente.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
6	**SUMINISTRO DE LA INFORMACION PERSONAL**				
31	La información personal que se suministra al Titular o a quien éste autorice es de fácil lectura, sin barreras técnicas que impidan su acceso y corresponde en un todo a aquella que reposa en la base de datos.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
32	Se suministra únicamente información personal a los Titulares, sus causahabientes o Sus representantes legales, a las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial y a los terceros autorizados por el Titular o por la ley.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
7	**ATENCION DE CONSULTAS Y RECLAMOS DE LOS TITULARES**				
33	Se cuenta con canales o mecanismos sencillos y ágiles y que estén permanentemente habilitados para la atención	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales

	de las consultas y reclamos de los Titulares o sus causahabientes.				
34	Se dan a conocer a los Titulares e interesados los canales habilitados para la atención de consultas y reclamos en la política de Tratamiento de datos personales dispuesta por la organización,	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
35	Se atiende, dentro de los diez (10) días hábiles contados a partir de su recibo, las consultas de información personal presentadas por los Titulares, sus causahabientes y las personas autorizadas.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
36	Se informa a los peticionarios el motivo de la no atención oportuna a su consulta de información personal y se señala la fecha de respuesta de la solicitud, sin exceder el término de cinco (5) días adicionales a los diez (10) días iniciales para contestar.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
37	Se atiende, dentro de los quince (15) días hábiles contados a partir de su recibo, las reclamaciones presentadas por los Titulares o sus causahabientes que consideran que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto Incumplimiento de cualquiera de los deberes contenidos en la ley.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
38	Se informa a los peticionarios el motivo de la no atención oportuna a su reclamo y se señala la fecha de respuesta de la solicitud, sin exceder el término de ocho (8) días adicionales a los quince (15) días Iniciales para contestar.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
39	Se adoptan medidas para asegurar que os datos personales que reposan en las bases de datos sean precisos y suficientes y, cuando así lo solicite el Titular o cuando haya podido advertirlo, sean actualizados,	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales

	rectificados o suprimidos, de tal manera que satisfagan los propósitos del Tratamiento.				
40	Se ha designado a una persona o área para que asuma la función de protección de datos personales y dé trámite a las solicitudes de los Titulares para el ejercicio de sus derechos.	SI ISO 27001	8.1	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
41	Se da a conocer a los Titulares los procedimientos dispuestos por la organización para el acceso, actualización, supresión y rectificación de datos personales y de revocatoria de la autorización, y los mismos son fácilmente accesibles.	SI ISO 27001	7.4	A12.1.1	Documentación de procedimientos operacionales
42	Se incluye dentro de la política de Tratamiento de datos personales los procedimientos dispuestos para garantizar el acceso, actualización, supresión y rectificación de datos personales y de revocatoria de la autorización.	SI ISO 27001	5.2	A12.1.1	Documentación de procedimientos operacionales
43	43. Se cuenta con un manual interno de políticas y procedimientos para garantizar la atención de consultas y reclamos presentados por los Titulares y para garantizar, en general, el adecuado cumplimiento de la ley.	SI ISO 27001	8.1	A12.1.1	Documentación de procedimientos operacionales
44	44. Se han adoptado procesos para la atención y respuesta a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto del Tratamiento de sus datos personales.	SI ISO 27001	8.1	A12.1.1	Documentación de procedimientos operacionales
8	**POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES**				
45	Se cuenta con una política para el Tratamiento de los datos personales.	SI ISO 27001	5.2	A5.1.2	Políticas para la seguridad de la información

46	La política para el Tratamiento de datos personales consta en medio físico o electrónico, en un lenguaje claro y sencillo, y es puesta en conocimiento de los Titulares.	SI ISO 27001	5.2	A5.1.2	Políticas para la seguridad de la información
47	Se cuenta con una política para el Tratamiento de datos personales que incluye el nombre o razón social, domicilio, dirección, correo electrónico y teléfono de la organización.	SI ISO 27001	5.2	A5.1.2	Políticas para la seguridad de la información
48	La política para el tratamiento de datos adoptada por la organización incluye información sobre el Tratamiento al cual serán sometidos los datos personales y a finalidad del mismo.	SI ISO 27001	5.2	A5.1.2	Políticas para la seguridad de la información
49	Incluye la política para el tratamiento de datos personales información sobre los derechos que le asisten a los Titulares respecto de su información personal.	SI ISO 27001	5.2	A5.1.2	Políticas para la seguridad de la información
50	Se informa en la política para el Tratamiento de datos personales sobre la persona o área Responsable de la atención de peticiones, consultas y reclamos ante la cual el Titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.	SI ISO 27001	5.2	A5.1.2	Políticas para la seguridad de la información
51	Se indica en la política para el Tratamiento de datos personales cuál o cuáles son los procedimientos para que los Titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización.	SI ISO 27001	5.2	A5.1.2	Políticas para la seguridad de la información
52	En la política para el Tratamiento de datos personales está Incluida la fecha de entrada en vigencia y el período de vigencia de la o las bases de datos que tiene la organización.	SI ISO 27001	5.2	A5.1.2	Políticas para la seguridad de la información
9	**AVISO DE PRIVACIDAD**				

53	Se informa a los Titulares la existencia de políticas para el tratamiento de datos personales por medio de un aviso de privacidad.	SI ISO 27001	7.4	A5.1.2	Políticas para la seguridad de la información
54	El aviso de privacidad publicado por la organización incluye el nombre o razón social y los datos de contacto de la misma.	SI ISO 27001	7.4	A5.1.2	Políticas para la seguridad de la información
55	En el aviso de privacidad publicado se incluye la descripción del tratamiento al cual serán sometidos los datos personales recolectados y la finalidad de tal recolección.	SI ISO 27001	7.4	A5.1.2	Políticas para la seguridad de la información
56	El aviso de privacidad incluye un listado de los derechos que tienen los Titulares cuya información es recolectada por la organización.	SI ISO 27001	7.4	A5.1.2	Políticas para la seguridad de la información
57	Se informa a los Titulares en el aviso de privacidad publicado, cómo acceder o consultar la política de Tratamiento de datos personales dispuesta por la organización.	SI ISO 27001	7.4	A5.1.2	Políticas para la seguridad de la información
58	En el aviso de privacidad publicado se señala expresamente la facultad que tienen los Titulares de contestar o no las preguntas que versen sobre datos personales sensibles o sobre los datos de niños, niñas y adolescentes.	SI ISO 27001	7.4	A5.1.2	Políticas para la seguridad de la información
59	Se conserva el modelo de aviso de privacidad utilizado para cumplir con la obligación legal de dar a conocer las políticas de Tratamiento de la información personal.	SI ISO 27001	7.4	A5.1.2	Políticas para la seguridad de la información
10	**REPORTE DE VIOLACIONES A LOS CÓDIGOS DE SEGURIDAD**				
60	Informa a la Superintendencia cuando se presentan violaciones a los códigos de seguridad que generen riesgos en la	SI ISO 27001	7.4	A16.1.1	Responsabilidades y procedimientos

	administración de la información de los Titulares.				
11	**GESTIÓN DE ENCARGADOS DEL TRATAMIENTO**				
61	Se han establecido procedimientos internos para asegurar que los encargados del Tratamiento garanticen la protección de los datos personales que le son entregados y que su Tratamiento se haga acorde con los principios y deberes establecidos en la ley.	SI ISO 27001	6.1.3	A13.2.1	Políticas y procedimientos de intercambio de información
62	Se suscriben contratos con los encargados que incluyan expresamente el tratamiento que éste podrá realizar a los datos personales.	SI ISO 27001	6.1.3	A13.2.2	Acuerdos de intercambio de información
63	Se suscriben contratos con los Encargados que incluyan cláusulas de confidencialidad de la Información entregada.	SI ISO 27001	6.1.3	A13.2.2	Acuerdos de intercambio de información
64	Se exige a los Encargados tener y mantener políticas de seguridad de la información y de Tratamiento de datos personales antes de entregar las bases de datos.	SI ISO 27001	6.1.3	A13.2.1	Políticas y procedimientos de intercambio de información
65	Se Informa al Encargado de forma oportuna todas las novedades respecto de los datos que previamente le fueron suministradas.	SI ISO 27001	6.1.3	A13.2.1	Políticas y procedimientos de intercambio de información
66	Se cuenta con medidas necesarias para que la información suministrada al Encargado se mantenga actualizada.	SI ISO 27001	6.1.3	A13.2.1	Políticas y procedimientos de intercambio de información
67	Se comunica al Encargado cuando se ha rectificado la información Incorrecta	SI ISO 27001	6.1.3	A13.2.1	Políticas y procedimientos de intercambio de información
68	Se comunica al Encargado si determinada información se encuentra en discusión por parte del Titular, una vez éste presenta una	SI ISO 27001	6.1.3	A13.2.1	Políticas y procedimientos de intercambio de información

	reclamación y no ha finalizado el trámite respectivo.				
69	Se verifica que el Encargado actualice y rectifique la información personal en los términos legales.	SI ISO 27001	6.1.3	A13.2.1	Políticas y procedimientos de intercambio de información
12	**TRANSFERENCIA Y TRANSMISIÓN INTERNACIONAL DE DATOS PERSONALES**				
70	Se transfieren datos personales a países que garantizan niveles adecuados de protección de datos, según lo establecido en el numeral del Capítulo Tercero del Título V de la Circular Única de la Superintendencia de industria y comercio.	SI ISO 27001	6.1.1	A13.2.1	Políticas y procedimientos de intercambio de información
71	Se han implementado medidas apropiadas y efectivas para garantizar el adecuado Tratamiento de los datos personales que se transfieren a otro país y para otorgar seguridad a los registros al momento de efectuar dicha transferencia.	SI ISO 27001	6.1.1	A13.2.1	Políticas y procedimientos de intercambio de información
72	Se transfieren datos personales fuera del territorio colombiano con base en alguna de las causales de excepción establecidas en el artículo 26 de la Ley 1581 de 2012	SI ISO 27001	6.1.1	A13.2.1	Políticas y procedimientos de intercambio de información
73	Se transfieren datos personales fuera del territorio colombiano con base en una declaración de conformidad emitida por esta Superintendencia.	SI ISO 27001	6.1.1	A13.2.1	Políticas y procedimientos de intercambio de información
74	Se han suscrito contratos con los Responsables del Tratamiento destinatarios de los datos personales a transferir fuera del territorio colombiano o se implementan otros instrumentos jurídicos en los que señalen las condiciones que regirán la transferencia internacional de datos personales, mediante	SI ISO 27001	6.1.1	A13.2.2	Acuerdos de intercambio de información

	las cuales se garantizará el cumplimiento de los principios que rigen el Tratamiento, así como de las obligaciones que tienen a cargo.				
75	Se transmiten datos personales fuera del territorio colombiano a un encargado para que realice el Tratamiento indicado por la organización como Responsable del Tratamiento y para ello se han suscrito contratos de transmisión de datos personales en los que se señalen los alcances del Tratamiento, las actividades que el encargado realizará y las obligaciones de este respecto de los Titulares y el Responsable.	SI ISO 27001	6.1.1	A13.2.1	Políticas y procedimientos de intercambio de información
76	Se incluyen en el contrato de transmisión internacional de datos personales celebrado con el Encargado cláusulas mediante las cuales este se compromete a dar aplicación a las obligaciones del Responsable bajo Su política de Tratamiento de la información y a realizar el Tratamiento de datos de acuerdo con la finalidad que los Titulares han autorizado y con las leyes aplicables.	SI ISO 27001	6.1.1	A13.2.2	Acuerdos de intercambio de información
77	Se incluye en el contrato de transmisión internacional de datos personales celebrado con el Encargado la obligación de dar Tratamiento, a nombre del Responsable, a los datos personales conforme a los principios establecidos en la ley general de protección de datos personales.	SI ISO 27001	6.1.1	A13.2.2	Acuerdos de intercambio de información
78	Se incluye en el contrato de transmisión internacional de datos personales celebrado con el Encargado la obligación para este de salvaguardar la seguridad de las bases de datos que contengan datos personales.	SI ISO 27001	6.1.1	A13.2.2	Acuerdos de intercambio de información

79	Se incluye en el contrato de transmisión internacional de datos personales celebrado con el Encargado la obligación para este de guardar confidencialidad respecto del Tratamiento de los datos personales.	SI ISO 27001	6.1.1	A13.2.2	Acuerdos de intercambio de información
13	**RESPONSABILIDAD DEMOSTRADA**				
80	80. Se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y el Decreto Único 1074 de 2015 de manera proporcional a la naturaleza jurídica de la organización y su tamaño empresarial.	SI ISO 27001	4.4	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
81	81. Se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y el Decreto único 1074 de 2015 de manera proporcional a la naturaleza de los datos personales Objeto del Tratamiento.	SI ISO 27001	4.4	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
82	82. Se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y el Decreto Único 1074 de 2015 de manera proporcional al tipo de Tratamiento que realice con los datos personales.	SI ISO 27001	4.4	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
83	83. Se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y el Decreto Único 1074 de 2015 de manera proporcional a los riesgos potenciales que el Tratamiento podría causar sobre los derechos de los Titulares.	SI ISO 27001	4.4	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
84	84. Se conserva evidencia sobre la implementación efectiva de medidas de seguridad apropiadas para el cumplimiento	SI ISO 27001	4.4	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales

	del régimen de protección de datos personales.				
85	85. Se han adoptado mecanismos internos para poner en práctica las políticas establecidas en los que se incluyan herramientas de implementación, entrenamiento y programas de educación en materia de protección de datos personales.	SI ISO 27001	4.4	A.18.1	Identificación de la legislación aplicable y de los requisitos contractuales
14	**REGISTRO NACIONAL DE BASES DE DATOS**				
86	86. Se han registrado las bases de datos con información personal de la organización en el Registro Nacional de Bases de Datos (RNBD), administrado por la Superintendencia de Industria y Comercio	SI ISO 27001	7.5.3	A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales
		86			

Nota. Datos obtenidos de la Ley 1581 de Protección de Datos Personales y la Norma ISO 27001.

Anexo 5. Anexo A de la Norma ISO 27001:2013

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado
A5	**Políticas de seguridad de la información**	
A5.1	**Directrices de gestión de la seguridad de la información**	
A5.1.1	Políticas para la seguridad de la información	Definido
A5.1.2	Revisión de las políticas para la seguridad de la información	Inexistente
A6	**Organización de la seguridad de la información**	
A6.1	**Organización interna**	
A6.1.1	Roles y responsabilidades en seguridad de la información	Definido
A6.1.2	Segregación de tareas	Definido
A6.1.3	Contacto con las autoridades	Inexistente
A6.1.4	Contacto con grupos de interés especial	Inexistente
A6.1.5	Seguridad de la información en la gestión de proyectos	Inexistente
A6.2	**Los dispositivos móviles y el teletrabajo**	
A6.2.1	Política de dispositivos móviles	Inexistente
A6.2.2	Teletrabajo	No aplicable
A7	**Seguridad relativa a los recursos humanos**	

A7.1	**Antes del empleo**	
A7.1.1	Investigación de antecedentes	Inicial
A7.1.2	Términos y condiciones del empleo	? Desconocido
A7.2	**Durante el empleo**	
A7.2.1	Responsabilidades de gestión	? Desconocido
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	? Desconocido
A7.2.3	Proceso disciplinario	? Desconocido
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**	
A7.3.1	Responsabilidades ante la finalización o cambio	? Desconocido
A8	**Gestión de activos**	
A8.1	**Responsabilidad sobre los activos**	
A8.1.1	Inventario de activos	? Desconocido
A8.1.2	Propiedad de los activos	? Desconocido
A8.1.3	Uso aceptable de los activos	? Desconocido
A8.1.4	Devolución de activos	? Desconocido
A8.2	**Clasificación de la información**	
A8.2.1	Clasificación de la información	? Desconocido
A8.2.2	Etiquetado de la información	? Desconocido
A8.2.3	Manipulado de la información	? Desconocido
A8.3	**Manipulación de los soportes**	
A8.3.1	Gestión de soportes extraíbles	? Desconocido
A8.3.2	Eliminación de soportes	? Desconocido
A8.3.3	Soportes físicos en tránsito	? Desconocido

A9	**Control de acceso**	
A9.1	**Requisitos de negocio para el control de acceso**	
A9.1.1	Política de control de acceso	? Desconocido
A9.1.2	Acceso a las redes y a los servicios de red	? Desconocido
A9.2	**Gestión de acceso de usuario**	
A9.2.1	Registro y baja de usuario	? Desconocido
A9.2.2	Provisión de acceso de usuario	? Desconocido
A9.2.3	Gestión de privilegios de acceso	? Desconocido
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	? Desconocido
A9.2.5	Revisión de los derechos de acceso de usuario	? Desconocido
A9.2.6	Retirada o reasignación de los derechos de acceso	? Desconocido
A9.3	**Responsabilidades del usuario**	
A9.3.1	Uso de la información secreta de autenticación	? Desconocido
A9.4	**Control de acceso a sistemas y aplicaciones**	
A9.4.1	Restricción del acceso a la información	? Desconocido
A9.4.2	Procedimientos seguros de inicio de sesión	? Desconocido
A9.4.3	Sistema de gestión de contraseñas	? Desconocido
A9.4.4	Uso de utilidades con privilegios del sistema	? Desconocido
A9.4.5	Control de acceso al código fuente de los programas	? Desconocido
A10	**Criptografía**	
A10.1	**Controles criptográficos**	
A10.1.1	Política de uso de los controles criptográficos	? Desconocido
A10.1.2	Gestión de claves	? Desconocido

A11	**Seguridad física y del entorno**	
A11.1	**Áreas seguras**	
A11.1.1	Perímetro de seguridad física	? Desconocido
A11.1.2	Controles físicos de entrada	? Desconocido
A11.1.3	Seguridad de oficinas, despachos y recursos	? Desconocido
A11.1.4	Protección contra las amenazas externas y ambientales	? Desconocido
A11.1.5	El trabajo en áreas seguras	? Desconocido
A11.1.6	Áreas de carga y descarga	? Desconocido
A11.2	**Seguridad de los equipos**	
A11.2.1	Emplazamiento y protección de equipos	? Desconocido
A11.2.2	Instalaciones de suministro	? Desconocido
A11.2.3	Seguridad del cableado	? Desconocido
A11.2.4	Mantenimiento de los equipos	? Desconocido
A11.2.5	Retirada de materiales propiedad de la empresa	? Desconocido
A11.2.6	Seguridad de los equipos fuera de las instalaciones	? Desconocido
A11.2.7	Reutilización o eliminación segura de equipos	? Desconocido
A11.2.8	Equipo de usuario desatendido	? Desconocido
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	? Desconocido
A12	**Seguridad de las operaciones**	
A12.1	**Procedimientos y responsabilidades operacionales**	
A12.1.1	Documentación de procedimientos operacionales	? Desconocido
A12.1.2	Gestión de cambios	? Desconocido
A12.1.3	Gestión de capacidades	? Desconocido

A12.1.4	Separación de los recursos de desarrollo, prueba y operación	? Desconocido
A12.2	**Protección contra el software malicioso (malware)**	
A12.2.1	Controles contra el código malicioso	? Desconocido
A12.3	**Copias de seguridad**	
A12.3.1	Copias de seguridad de la información	? Desconocido
A12.4	**Registros y supervisión**	
A12.4.1	Registro de eventos	? Desconocido
A12.4.2	Protección de la información del registro	? Desconocido
A12.4.3	Registros de administración y operación	? Desconocido
A12.4.4	Sincronización del reloj	? Desconocido
A12.5	**Control del software en explotación**	
A12.5.1	Instalación del software en explotación	? Desconocido
A12.6	**Gestión de la vulnerabilidad técnica**	
A12.6.1	Gestión de las vulnerabilidades técnicas	? Desconocido
A12.6.2	Restricción en la instalación de software	? Desconocido
A12.7	**Consideraciones sobre la auditoria de sistemas de información**	
A12.7.1	Controles de auditoría de sistemas de información	? Desconocido
A13	**Seguridad de las comunicaciones**	
A13.1	**Gestión de la seguridad de las redes**	
A13.1.1	Controles de red	? Desconocido
A13.1.2	Seguridad de los servicios de red	? Desconocido
A13.1.3	Segregación en redes	? Desconocido
A13.2	**Intercambio de información**	
A13.2.1	Políticas y procedimientos de intercambio de información	? Desconocido

A13.2.2	Acuerdos de intercambio de información	? Desconocido
A13.2.3	Mensajería electrónica	? Desconocido
A13.2.4	Acuerdos de confidencialidad o no revelación	? Desconocido
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**	
A14.1	**Requisitos de seguridad en los sistemas de información**	
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	? Desconocido
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	? Desconocido
A14.1.3	Protección de las transacciones de servicios de aplicaciones	? Desconocido
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**	
A14.2.1	Política de desarrollo seguro	? Desconocido
A14.2.2	Procedimiento de control de cambios en sistemas	? Desconocido
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	? Desconocido
A14.2.4	Restricciones a los cambios en los paquetes de software	? Desconocido
A14.2.5	Principios de ingeniería de sistemas seguros	? Desconocido
A14.2.6	Entorno de desarrollo seguro	? Desconocido
A14.2.7	Externalización del desarrollo de software	? Desconocido
A14.2.8	Pruebas funcionales de seguridad de sistemas	? Desconocido
A14.2.9	Pruebas de aceptación de sistemas	? Desconocido
A14.3	**Datos de prueba**	
A14.3.1	Protección de los datos de prueba	? Desconocido
A15	**Relación con proveedores**	
A15.1	**Seguridad en las relaciones con proveedores**	
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	? Desconocido
A15.1.2	Requisitos de seguridad en contratos con terceros	? Desconocido

A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	? Desconocido
A15.2	**Gestión de la provisión de servicios del proveedor**	
A15.2.1	Control y revisión de la provisión de servicios del proveedor	? Desconocido
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	? Desconocido
A16	**Gestión de incidentes de seguridad de la información**	
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**	
A16.1.1	Responsabilidades y procedimientos	? Desconocido
A16.1.2	Notificación de los eventos de seguridad de la información	? Desconocido
A16.1.3	Notificación de puntos débiles de la seguridad	? Desconocido
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	? Desconocido
A16.1.5	Respuesta a incidentes de seguridad de la información	? Desconocido
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	? Desconocido
A16.1.7	Recopilación de evidencias	? Desconocido
A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**	
A17.1	**Continuidad de la seguridad de la información**	
A17.1.1	Planificación de la continuidad de la seguridad de la información	? Desconocido
A17.1.2	Implementar la continuidad de la seguridad de la información	? Desconocido
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	? Desconocido
A17.2	**Redundancias**	
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	? Desconocido
A18	**Cumplimiento**	
A18.1	**Cumplimiento de los requisitos legales y contractuales**	

A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	? Desconocido
A18.1.2	Derechos de Propiedad Intelectual (DPI)	? Desconocido
A18.1.3	Protección de los registros de la organización	? Desconocido
A18.1.4	Protección y privacidad de la información de carácter personal	? Desconocido
A18.1.5	Regulación de los controles criptográficos	? Desconocido
A18.2	**Revisiones de la seguridad de la información**	
A18.2.1	Revisión independiente de la seguridad de la información	? Desconocido
A18.2.2	Cumplimiento de las políticas y Normas de seguridad	? Desconocido
A18.2.3	Comprobación del cumplimiento técnico	? Desconocido

Anexo 6. *Validación de Expertos mediante formato de evaluación*

INSTRUMENTO DE VALIDACIÓN

ESCALA DE VALORACIÓN DE LA VARIABLE DEPENDIENTE: CUMPLIMIENTO DE LA LEY 1581 DE 2012

INSTRUCCIÓN: Sírvase encerrar dentro de un círculo, el número (representa porcentaje) que crea conveniente para cada pregunta.

1. ¿Considera usted que el diseño automatizado del SGSI basado en la norma ISO 27001:2013 mediante el sistema Eramba cumple el objetivo propuesto?

0 10 20 30 40 50 60 70 80 90 (100)

2. ¿Considera usted que el diseño automatizado del SGSI basado en la norma ISO 27001:2013 mediante el sistema Eramba contiene los conceptos propios del tema que se investiga?

0 10 20 30 40 50 60 70 80 90 (100)

3. ¿Estima usted que los controles que contiene el diseño automatizado del SGSI basado en la norma ISO 27001:2013 mediante el sistema Eramba son suficientes para dar cumplimiento a la protección de los datos personales según la Ley 1581 de 2012?

0 10 20 30 40 50 60 70 80 90 (100)

4. ¿Considera usted que el diseño automatizado del SGSI basado en la norma ISO 27001:2013 mediante el sistema Eramba en otro contexto cumpliría el objetivo del cumplimiento de la Ley 1581 de protección de datos personales?

0 10 20 30 40 50 60 70 80 90 (100)

5. ¿Qué controles de seguridad cree usted que se podrían agregar al sistema Eramba?

Ninguno

6. ¿Qué controles de seguridad cree usted que se podrían eliminar?

Ninguno

Validado por: JAIME BLANCO LÓPEZ

Grado académico: (Doctor en la línea) CIENCIAS DE LA COMPUTACIÓN

Universidad: UNIVERSIDAD CENTRAL DE VENEZUELA

(aquí va el nombre de la universidad donde estudio el experto su último grado)

INSTRUMENTO DE VALIDACIÓN

ESCALA DE VALORACIÓN DE LA VARIABLE DEPENDIENTE: CUMPLIMIENTO DE LA LEY 1581 DE 2012

INSTRUCCIÓN: Sírvase encerrar dentro de un círculo, el número (representa porcentaje) que crea conveniente para cada pregunta.

1. ¿Considera usted que el diseño automatizado del SGSI basado en la norma ISO 27001:2013 mediante el sistema Eramba cumple el objetivo propuesto?

0 10 20 30 40 50 60 70 80 90 (100)

2. ¿Considera usted que el diseño automatizado del SGSI basado en la norma ISO 27001:2013 mediante el sistema Eramba contiene los conceptos propios del tema que se investiga?

0 10 20 30 40 50 60 70 80 90 (100)

3. ¿Estima usted que los controles que contiene el diseño automatizado del SGSI basado en la norma ISO 27001:2013 mediante el sistema Eramba son suficientes para dar cumplimiento a la protección de los datos personales según la Ley 1581 de 2012?

0 10 20 30 40 50 60 70 80 90 (100)

4. ¿Considera usted que el diseño automatizado del SGSI basado en la norma ISO 27001:2013 mediante el sistema Eramba en otro contexto cumpliría el objetivo del cumplimiento de la Ley 1581 de protección de datos personales?

0 10 20 30 40 50 60 70 80 90 (100)

5. ¿Qué controles de seguridad cree usted que se podrían agregar al sistema Eramba?

Ninguno, porque todos los Controles que pide la ley están contemplados en el SGSI

6. ¿Qué controles de seguridad cree usted que se podrían eliminar?

Ninguno, porque todos los Controles de SGSI son necesarios para el Cumplimiento de la ley

Validado por: Daniel Castillo

Grado académico: (Magíster en la línea) Ingeniería de Sistemas

Universidad: UPEV.

(aquí va el nombre de la universidad donde estudio el experto su último grado)