Modelo de Sistema de Gestión de Seguridad de la Información Basado en la Norma NTC ISO/IEC 27001 para Instituciones Públicas de Educación Básica de la Comuna Universidad de la Ciudad de Pereira

Alejandra María Benavides Sepúlveda & Carlos Arturo Blandón Jaramillo

Universidad Autónoma de Manizales
Facultad de Ingeniería de Sistemas
Maestría en Gestión y Desarrollo de Proyectos de Software
Manizales, Colombia

Cohorte VI
2017

Modelo de Sistema de Gestión de Seguridad de la Información Basado en la Norma NTC ISO/IEC 27001 para Instituciones Públicas de Educación Básica de la Comuna Universidad de la Ciudad de Pereira

Alejandra María Benavides Sepúlveda & Carlos Arturo Blandón Jaramillo

Proyecto para optar al título de:

Magister en Gestión y Desarrollo de Proyectos de Software

Director:

PhD Francisco Javier Valencia Duque

Énfasis:

Gestión

Universidad Autónoma de Manizales

Facultad de Ingeniería de Sistemas

Manizales, Colombia

2017

Dedicatoria

A Dios por dotarme de paciencia y fortaleza para superar los obstáculos afrontados durante esta etapa de mi vida.

A mis padres María y Jairo por sus amorosas enseñanzas, y su constante aliento para asumir con responsabilidad este reto para lograr mi crecimiento personal y profesional.

A Juan Carlos por sus palabras, paciencia y constante apoyo contribuyendo al logro mis objetivos.

Alejandra María.

A Dios por haberme permitido culminar esta etapa, concediéndome salud para lograr mis objetivos y paciencia para no rendirme en la mitad del camino.

A mi madre Enohe por sus consejos, sus valores, su motivación, perseverancia y constancia que la caracterizan que me ha infundido siempre permitiéndome ser una persona de bien, pero ante todo por su amor incondicional que me llena de júbilo y regocijo.

Carlos Arturo

Agradecimientos

Queremos agradecer profundamente al Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, en virtud al apoyo recibido a través de la convocatoria de Talento Digital que nos permitió acceder a formación de nivel de postgrado, de igual manera extendemos nuestros agradecimientos a la Universidad Autónoma de Manizales y a todo su personal por el apoyo brindado en el proceso tanto administrativo como académico, así mismo a las instituciones educativas de la Comuna Universidad y de la Comuna San Fernando de la ciudad de Pereira departamento de Risaralda, por abrirnos las puertas de sus instalaciones, brindarnos la confianza y proporcionarnos el personal y material necesarios para el desarrollo de nuestro trabajo.

De igual manera agradecemos a nuestro asesor Francisco Javier Valencia Duque por su esfuerzo y dedicación, sus orientaciones, su manera de trabajar, su persistencia, su paciencia y su motivación que fueron fundamentales en nuestra formación investigativa.

Tabla de contenido

Lista de Tablas

Lista de Gráficas

Resumen

El avance tecnológico de los sistemas de información tanto a nivel de hardware como de software tendientes a la ubicuidad se han convertido en un pilar fundamental para garantizar la continuidad y competitividad de las organizaciones en un mercado cada vez más exigente en términos de calidad, oportunidad y seguridad tanto del servicio como de la información relacionada, procurando el cumplimiento de los criterios de seguridad de la información asegurando su integridad, seguridad y confidencialidad.

En aras del cumplimiento de estos criterios, en las instituciones del sector público el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC ha establecido las directrices generales que permiten implementar Sistemas de Gestión de Seguridad de la Información – SGSI buscando el acercamiento del estado con la ciudadanía, brindando seguridad en las transacciones, confianza y oportunidad en la prestación de servicios.

La educación básica es un servicio que ofrece el estado, y a la vez un derecho de los niños y niñas consagrado en la Constitución política de Colombia, el cual se encuentra circunscrito en el Decreto Reglamentario 1078 de mayo de 2015 el cual establece los lineamientos para la implementación de la Estrategia de Gobierno en Línea en todas las entidades públicas colombianas, incluyendo el establecimiento de un SGSI basado en la Norma Internacional NTC/ISO IEC 27001.

La presente tesis tiene como fin proponer un modelo que facilite la Implementación del SGSI en Instituciones Educativas – IED’s que presten servicios educativos de básica, en armonía con los requerimientos establecidos por el Ministerio de Educación Nacional, MINTIC y las necesidades propias de las IED’s.

Abstract

The technological advance of both hardware and software information systems aimed at ubiquity have become a fundamental pillar to ensure the continuity and competitiveness of organizations in an increasingly demanding market in terms of quality, opportunity and security of both the service and the related information, ensuring compliance with the criteria of information security, guaranteeing its Integrity, Security and Confidentiality.

In order to comply with these criteria in public sector institutions, the Ministry of Information Technologies and Communications - MINTIC has established the general guidelines that allow the implementation of Information Security Management Systems - ISMS seeking to bring the State closer to Citizenship, providing security in the transactions, trust and opportunity in the provision of services.

Basic education is a service provided by the State, and at the same time a right of the boys and girls consecrated in the Political Constitution of Colombia, which is circumscribed in Regulatory Decree 1078 of May of 2015 which establishes the guidelines for the implementation of the Online Government Strategy, including the establishment of an ISMS based on the International Standard NTC / ISO IEC 27001.

The present thesis intends to propose a model that facilitates the Implementation of the ISMS in Educational Institutions - IEDs that provide Basic Educational Service in harmony with the requirements established by the Ministry of National Education, MINTIC and according to the own needs of the IEDs

Introducción

En las últimas décadas, el vertiginoso avance de las herramientas para el procesamiento de información (equipos de cómputo, dispositivos móviles, tablets, etc) tanto en el aspecto físico (hardware) como lógico (software), así como el desarrollo de los mecanismos empleados para establecer comunicaciones, han generado dinamismo en los procesos productivos y de prestación de servicios, pero de igual manera han surgido riesgos a la seguridad de la información, producto de dichos avances contrastados con la poca preparación de las organizaciones que adoptan estas tecnologías como elementos esenciales para el desarrollo de las actividades de los procesos organizacionales.

Acorde con este avance tecnológico y descubrimiento de nuevos riesgos a la seguridad de la información, se han desarrollado y actualizado diversas guías de buenas prácticas en la administración de los activos de información, que se convierten en estrategias adoptadas por las organizaciones para la preservación de la confidencialidad, integridad y disponibilidad de la información.

Las entidades del estado en cumplimiento del decreto reglamentario 1078 de 2015, deben implementar un SGSI que garantice los aspectos antes mencionados, para lo cual MINTIC ha desarrollado una serie de guías que sirven de base para cumplir con este objetivo y que son de libre uso por parte de las organizaciones que cumplen funciones públicas y que les permiten ser más competitivas en el mundo globalizado en el cual las exigencias son cada vez mayores.

(Velásquez Isaza, 2015), afirma:

> Es clara la brecha existente entre la tecnología y la manera como se realiza de manera segura las operaciones al interior de la organización para garantizar la confidencialidad, disponibilidad e integridad de esa información que pasa, en la mayoría de los casos, por

manos de uno, dos o más empleados sin tomar las medidas adecuadas para su correcto tratamiento. (p.19)

En la presente tesis se realizó la construcción de un modelo de SGSI basado en la norma NTC ISO/IEC 27001:2013 para instituciones públicas de educación básica de la ciudad de Pereira, cuyo alcance está determinado por el área de Secretaria Académica, tomando como población objeto de estudio aquellas Instituciones Educativas – IED's que se encuentran localizadas en la Comuna Universidad y San Fernando de la ciudad de Pereira en el departamento de Risaralda.

Para lograr el objetivo propuesto se adelantó un diagnóstico inicial de brechas de cumplimiento en relación con los requisitos exigidos por la norma internacional ISO/IEC 27001:2013, que constituyeron el punto de partida para determinar el grado de madurez e implementación del SGSI, además se generó la declaración de aplicabilidad conforme a los controles establecidos en el Anexo A de la Norma ISO 27001:2013.

El objetivo del modelo de seguridad de la información propuesto es que se constituya en un esquema de fácil y detallada implementación para todas las IED´s, alineando el marco legal propio del sector educativo con el estándar internacional de seguridad de la información y los lineamiento trazados por MINTIC para tal fin, logrando a partir de ello, un fortalecimiento de la relación ciudadanía – estado, a través del cumplimiento de los propósitos de "encontrar diferentes formas para que la gestión de las entidades públicas sea óptima gracias al uso estratégico de la tecnología de la información y garantizar la seguridad y privacidad de la información", (MINTIC, 2015, pág. 2)

1. Referente Contextual

1.1.Área Problemática

La evolución dinámica de las tecnologías de información y comunicaciones han permeado las organizaciones públicas y privadas de tal manera que se han convertido en uno de los factores determinantes para el logro de los objetivos a corto, mediano y largo plazo, así como medio indispensable para la agilidad en la prestación del servicio, diversificación de los canales de atención al público, transparencia y la seguridad de la información entre otros[1].

Las entidades que cumplen funciones públicas en el estado colombiano de conformidad con lo expresado en la Ley 489 de 1998, dentro de las cuales se encuentran las entidades de orden nacional y territorial que prestan servicios a los ciudadanos que son responsabilidad del estado, no son ajenas a la inclusión de las nuevas tecnologías en los procesos organizacionales[2].

> El crecimiento en el uso masivo de las Tecnologías de la Información y Comunicaciones en Colombia, reflejado en la masificación de las redes de telecomunicaciones como base para cualquier actividad económica y el incremento en la oferta de servicios en línea, dan fe del aumento de la participación digital de los ciudadanos. (Departamento Nacional de Planeación, 2016, pág. 9).

Está dinámica digital genera incertidumbre y riesgos inherentes a las actividades relacionadas con la seguridad electrónica que requieren de atención oportuna y continuada, es así

---

[1] Como ejemplo, de acuerdo a la información suministrada por la Superintendencia Financiera de Colombia (2015), el número de operaciones financieras mediante el canal de internet aumentó en un 45% de 2012 a 2014 y mediante telefonía móvil un 252%.

[2] Según el programa de Gobierno en Línea el porcentaje de los ciudadanos colombianos que usan canales o medios electrónicos para (i) obtener información, (ii) realizar trámites, (iii) obtener servicios, (iv) presentar peticiones, quejas o reclamos, o (v) participar en la toma de decisiones, pasó del 30% en 2009 al 65% en 2014.

como el Ministerio de Tecnologías de la Información y Comunicaciones en procura de garantizar la confidencialidad, la integridad y disponibilidad de la información de las entidades del estado, ha generado políticas que permiten cerrar la brecha que en materia de seguridad digital se tiene actualmente.

El sector educativo se encuentra incluido en estas políticas, pero a la vez tiene requerimientos legales que particularizan las guías y mandatos del MINTIC en cuanto a las actividades que se encuentran en el decreto 1078/2015 titulo 9 para la implementación de un SGSI.

Se genera entonces la necesidad de alinear los requerimientos del MINTIC, el MEN y la Norma Internacional NTC ISO/IEC 27001:2013 en un modelo que permita su aplicación en las entidades educativas de nivel básica y carácter oficial, priorizando su desarrollo en el área de Secretaria Académica en virtud de la información gestionada en este proceso.

1.2.Antecedentes

(Novoa & Helena, 2015), describen detalladamente el procedimiento seguido para determinar los parámetros y lineamientos requeridos para la implementación de un SGSI para organizaciones dedicadas a la formación superior, se describen el alcance y las políticas del SGSI, así como las metodologías empleadas para llevar a cabo la valoración de los activos de información y análisis de riesgos.

(Aliaga Florez, 2013) por su parte, realiza un modelamiento detallado de los procesos “core” del instituto educativo, de igual manera se detalla la metodología seguida para la identificación y evaluación de riesgos y su respectivo mapeo con los controles de COBIT 5,

describiendo finalmente la declaración de aplicabilidad obtenida en el diseño del sistema de gestión.

(Irrazabal, Gómez, & Cardoso, 2013), dan una revisión general de la importancia que tiene la formación del recurso humano en seguridad de información, así como una explicación sucinta del rol que juegan las tecnologías de información y los sistemas de información dentro de las organizaciones.

(Espinosa T., Martinez P., & Amador D., 2014) hacen un análisis de la aplicación de la metodología OCTAVE-S, describiendo la estructura del proceso DARCA y el procedimiento seleccionado para llevar a cabo el tratamiento de los riesgos.

(Caviedes Sanabria & Prado Urrego, 2012), realizan una síntesis de la evolución de los marcos de trabajo COBIT, RiskIT, ISO27000, ISM3, ITIL, MoR, MagerIT, presentando en el mismo el sustento de la necesidad de generar modelos que indiquen de una manera más detallada las actividades que deben seguir las organizaciones en términos de las tareas asociadas a la valoración de los activos de información.

(Betancourt Correa, Posada Bonilla, & Rangel García, 2014), describen la metodología empleada para el diseño de un Sistema de Gestión de Seguridad de la Información para la Alcaldía de Manizales, brindando elementos importantes para la construcción del modelo, de igual manera presenta la gestión de riesgos seguida por los autores lo que permite dar mayor sustento teórico a la gestión de riesgos que se propuso en el modelo.

Lo anterior deja claro el interés de las organizaciones y de las entidades dedicadas a la implementación de SGSI en contar con un modelo que permita gestionar adecuadamente los riesgos. Sin embargo, en el sector de la educación y las entidades públicas en Colombia se presenta

una brecha que no permite garantizar la seguridad de la información de los jóvenes y docentes vinculados a estas instituciones.

1.3.Justificación

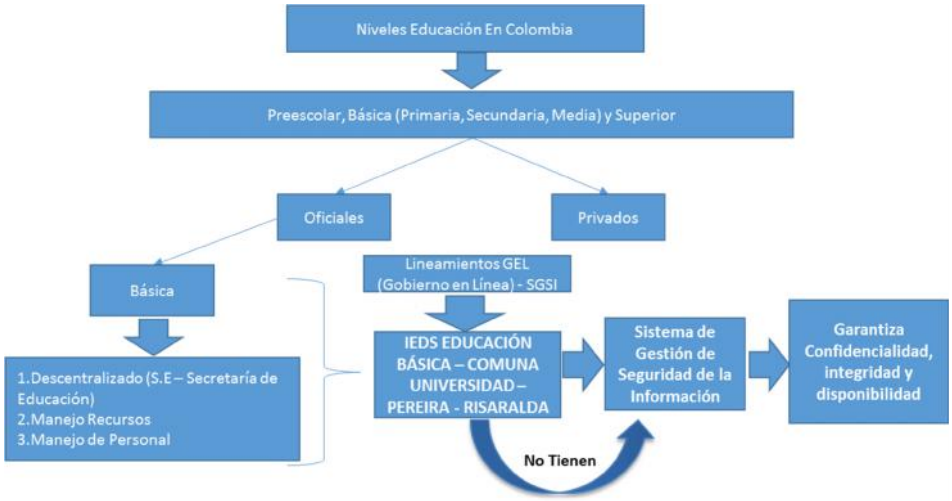
La educación básica en Colombia comprende los niveles de primaria, secundaria y media (Codesocial, 2009), ofrecidos por el estado colombiano a través de las Secretarías de Educación Departamentales y Municipales, a las cuales se encuentran vinculadas las Instituciones Educativas que llevan este servicio al contacto con el ciudadano, teniendo un modelo administrativo descentralizado lo que las hace autónomas en diversos aspectos relacionados con la gestión de recursos pero contraladas y vigiladas por la Secretaría de Educación a la cual pertenecen, tal como se observa en la gráfica 1. Estas entidades requieren implementar mecanismos que garanticen el servicio y la transparencia de cara al mundo cada vez más digital en el cual nos encontramos.

Como entidades que ejercen funciones públicas, y ejecutan presupuestos provenientes del erario público, deben acogerse al decreto 1078 de mayo de 2015, título 9, sección 2, artículo 2.2.9.1.2.1. Componentes, ítem 4 “Seguridad y privacidad de la información”, el cual pretende acercar el estado a los ciudadanos a través de la prestación del servicio transparente, de calidad y salvaguardando la confidencialidad, integridad y disponibilidad de la información.

Los beneficios generados por la implementación de un modelo de SGSI en estas entidades de orden territorial son los siguientes:

- Proporcionar un marco de referencia para el tratamiento del riesgo
- Impulsar la implementación sistemática del ciclo PHVA, conducente a la mejora continua.

- Procurar la disponibilidad del servicio
- Concientización de los colaboradores de la organización
- Disminución de los gastos asociados al tratamiento de incidentes de seguridad
- Aseguramiento del cumplimiento de las disposiciones legales y reglamentarias
- Aumento de la confianza de los stakeholders, acercando al ciudadano a los servicios públicos
- Incremento de la competitividad en términos de disponibilidad y seguridad de la información
- Alineación con los requisitos de la Norma NTC ISO 27001
- Documentación de las actividades propias de los procesos administrativos, que permitan la trazabilidad de las acciones tomadas en cada puesto de trabajo



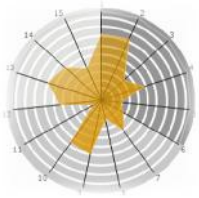
Gráfica 1. Representación de la estructura educativa en Colombia y los lineamientos de GEL

Fuente (León Zuluaga & Grajales Valencia , 2016)

Índices Estrategia de Gobierno en Línea sector educación

Los índices de medición de la estrategia de gobierno en línea desarrollados por MINTIC en el orden nacional, territorial e institucional, establecen como resultados lo siguiente:

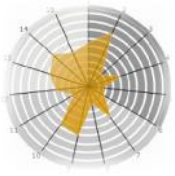
Orden nacional: “el subíndice Eficiencia Electrónica (Numerales del 1 al 5), tiene un puntaje de 22,05 para la implementación del SGSI (numeral 5) siendo el más bajo de las actividades relacionadas al sub índice”. (León Zuluaga & Grajales Valencia , 2016), como se observa en la gráfica 2, las instituciones educativas no tienen estrategias conducentes a la implementación de un Sistema de Gestión de Seguridad de la Información.



Gráfica 2. Medición implementación estrategia de GEL del orden nacional.

Fuente (MINTIC, 2015)

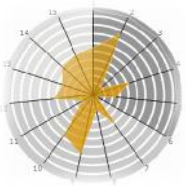
Orden territorial: “se evidencia que el Subíndice Eficiencia Electrónica (Numerales del 1 al 5, tiene un puntaje de 18,96 para la implementación del SGSI (numeral 5) siendo el más bajo de las actividades relacionadas al subíndice”, (León Zuluaga & Grajales Valencia , 2016), ver gráfica 3, a nivel nacional el Departamento de Risaralda se ubicó en el puesto 16.



Gráfica 3. Medición implementación estrategia de GEL de orden territorial.

Fuente: (MINTIC, 2015)

Orden interno Departamento de Risaralda: “en el Subíndice de Eficiencia Electrónica (Numerales del 1 al 5), tiene un puntaje de 26,26 para la implementación del SGSI ubicándolo de segundo dentro de las actividades del subíndice, (León Zuluaga & Grajales Valencia , 2016), Ver gráfica 4.



Gráfica 4. Medición implementación de la estrategia de GEL Departamento de Risaralda.

Fuente: (MINTIC, 2015)

Los resultados anteriores permiten evidenciar la carencia de acciones que permitan cerrar las brechas de cumplimiento de las instituciones de educación básica de carácter oficial, en torno a las disposiciones contenidas en el titulo 9 del Decreto 1078 de 2015.

1.4.Pregunta de investigación

¿Es posible asegurar la confidencialidad, integridad y disponibilidad de la información en las Instituciones Educativas de carácter público que prestan servicios educativos de nivel básico de la comuna Universidad de la Ciudad de Pereira, mediante un modelo que alinee los requerimientos de la estrategia de Gobierno en Línea con los requisitos de la norma NTC ISO/IEC 27001?

1.5.Objetivos

1.5.1. Objetivo general

Diseñar un modelo de Seguridad de la Información basado en la norma NTC ISO/IEC 27001 para asegurar la confidencialidad, integridad, disponibilidad y control de la información en instituciones públicas de educación básica de la ciudad de Pereira – Comuna Universidad.

1.5.2. Objetivos específicos

- Diagnosticar el grado de cumplimiento de la norma ISO 27001 en instituciones públicas de educación básica en el municipio de Pereira en la comuna Universidad.
- Identificar los controles requeridos para el tratamiento de los riesgos a la seguridad de información, de la Secretaría Académica de las instituciones públicas de educación básica de la Comuna Universidad de la Ciudad de Pereira.
- Diseñar la documentación el modelo del SGSI
- Validar el modelo en el área de secretaria académica de las IED’s Comuna Universidad y Comuna San Fernando de la Ciudad de Pereira

2. Estrategia Metodológica

2.1.Metodología

2.1.1. Tipo de estudio

La presente investigación tuvo enfoque cualitativo, que generalmente es empleado con el objetivo de descubrir preguntas de investigación en algunas ocasiones, pero no necesariamente se prueban hipótesis (Grinnel, 1997). Su propósito es abstraer la realidad, de la manera en la cual es percibida por las partes interesadas y que participan directa o indirectamente en el objeto de estudio.

La investigación adoptó este enfoque cualitativo dado que se buscaba generar buenas prácticas con base a los lineamientos dados por los organismos participantes (MINTIC, MEN, ISO), tendientes a garantizar la seguridad de la información dentro del contexto escolar, por lo tanto, los resultados se traducen en un modelo expresado en palabras y no en cifras.

Como punto inicial de la investigación se realizó la generación de un diagnóstico inicial en las instituciones educativas de nivel básico de carácter oficial que pertenecen a la Comuna Universidad y Comuna San Fernando de la ciudad de Pereira en el departamento de Risaralda, sin embargo, la unidad de trabajo definida en el alcance del proyecto es el área de Secretaría Académica de las IED´s.

2.1.2. Muestra y muestreo

En la presente investigación se realizó el diagnóstico inicial de brechas de cumplimiento normativo y grado de madurez de los SGSI en la totalidad de instituciones educativas de la Comuna Universidad; la validación del modelo propuesto se llevó a cabo en una institución de la Comuna Universidad y una de la comuna San Fernando de la ciudad de Pereira departamento de Risaralda, las cuales se relacionan en la tabla 1:

Tabla 1. Instituciones Educativas nivel básico de carácter oficial Comuna Universidad y la Comuna San Fernando de la Ciudad de Pereira.

Fuente: Secretaria de Educación Municipal - Pereira

Sujeto de estudio	Institución Educativa	Comuna
1	Colegio Remigio Antonio Cañarte	Universidad
2	Escuela Mariela Lemus Gutiérrez	Universidad
3	La Julita	Universidad
4	Técnico Superior	Universidad
5	San Fernando	San Fernando

En las instituciones educativas en las que se adelantó el proceso de validación del modelo planteado, se aplicó en el área de Secretaria Académica, la cual se determinó era el proceso más crítico, como resultado de las reuniones realizadas con los rectores de las IED´s, y para lo cual se tuvieron en cuenta los siguientes criterios, ver tabla 2:

Tabla 2. Factores para determinar la criticidad de los activos en las IED.

Criterio	Factor	Descripción
Confidencialidad	Financiero	Si el activo o información que se gestiona a través de él no están disponibles puede generar pérdidas económicas
	Legal	Si el activo o la información que se gestiona a través de él no están disponibles puede generar sanciones legales de las entidades de control o demandas de terceros

Criterio	Factor	Descripción
Integridad	Imagen Institucional	Si el activo o la información que se gestiona a través de él no están disponibles puede afectar la imagen de la entidad
	Financiero	Si el activo o la información que se gestiona a través de él son alterados sin autorización puede generar pérdidas económicas a la IED
	Legal	Si el activo o la información que se gestiona a través de él son alterados sin autorización puede generar sanciones de las entidades de control
	Imagen Institucional	Si el activo o la información que se gestiona a través de él son alterados sin autorización puede afectar la imagen
Disponibilidad	Financiero	Si la divulgación no autorizada puede revelar información sensible de la IED requerida para la debida administración y toma de decisiones.
	Legal	Si la divulgación no autorizada puede afectar el cumplimiento de regulaciones impartidas por entidades de control o puede generar demandas de terceros
	Imagen Institucional	Su divulgación no autorizada puede afectar la imagen

2.1.3. Técnicas e instrumentos de recolección de información

Se diseñaron los siguientes instrumentos:

1. Diagnóstico de brechas de cumplimiento de requisitos de la Norma ISO 27001:2013
2. Determinación de la criticidad de los activos de información

Adicionalmente, se aplicaron los siguientes instrumentos suministrados por MINTIC

1. Guía encuesta diagnóstico Modelo de Seguridad de la Información para las entidades del Estado
2. Modelo de seguridad de la información para la Estrategia de Gobierno en Línea
3. Guía técnica controles de seguridad y privacidad de la información
4. Guía técnica gestión de incidentes de seguridad de la información

2.1.4. Procedimientos

Para alcanzar los objetivos propuestos se ejecutaron las siguientes fases:

Fase 1: Caracterización de las IED

Se realizó la aplicación del instrumento de diagnóstico de brechas de cumplimiento de la Norma ISO/IEC 27001:2013, así como la guía técnica encuesta diagnóstico modelo de seguridad de la Información para las entidades del Estado propuesta por el MINTIC, está fase involucró actividades tales como:

1. Entrevistas con personal de las IED´s
2. Observación directa y toma de registro fotográfico
3. Aplicación de los instrumentos
4. Análisis de resultados

Fase 2: Análisis de riesgos

En esta fase se ejecutaron las siguientes actividades:

1. Determinación de la criticidad de los activos de información, mediante la aplicación del instrumento que permite priorizar dicha criticidad a través los factores financieros, legales e imagen de cada uno de los criterios de la seguridad de la información.
2. Determinación de los escenarios de riesgos para los activos críticos.
3. Determinación de los riesgos Inherentes
    a. Calificación del impacto para cada uno de los escenarios identificados.
    b. Calificación de la probabilidad para cada uno de los escenarios identificados.
    c. Calificación del impacto x probabilidad de cada uno de los escenarios identificados.

4. Elaboración de las matrices de temperatura de riesgos inherentes.

Fase 3: Selección de controles

1. Identificación de los controles apropiados para los riesgos inherentes.
2. Generación de la declaración de aplicabilidad.
3. Determinación de los riesgos residuales
    a. Calificación del impacto para cada uno de los escenarios identificados.
    b. Calificación de la probabilidad para cada uno de los escenarios identificados.
    c. Calificación del impacto x probabilidad de cada uno de los escenarios identificados.
4. Elaboración de las matrices de temperatura de riesgos residuales.

Fase 4: Diseño del modelo

1. Análisis de los requisitos legales del MINTIC referentes a la estrategia de Gobierno en Línea para las entidades del estado
2. Análisis de los requisitos legales del MINEDUCACIÓN, referentes al tratamiento de la información en las IED, así como los sistemas de información empleados
3. Diseño de los procedimientos y actividades detallados para construir el modelo de SGSI alineado con los requisitos legales del MINTIC, MINEDUCACION y el estado, así como los de la Norma ISO 27001:2013.

Fase 5: Selección de herramienta de consulta para el SGSI

1. Análisis de las plataformas de software GNU/GPL existentes, mediante la construcción de una matriz que determine las cualidades, prestaciones y requisitos de cada una de las herramientas analizadas.

2. Puesta a punto de la herramienta para la consulta del Modelo del SGSI propuesto.

Fase 6: Validación y socialización del modelo

1. Aplicación del modelo en el área de secretaria académica en las IED de la comuna Universidad.
2. Aplicación del modelo en el área de secretaria académica en la IED de la Comuna San Fernando.

2.1.5. Plan de análisis

El análisis de los resultados parciales y totales se adelantó por fases de la siguiente manera:

Fase 1: Caracterización de las IED´s

1. Interpretación de resultados obtenidos por el instrumento de diagnóstico de brechas de cumplimiento, mediante el uso de Microsoft Excel:
    a. Brecha total de cumplimiento normativo
    b. Porcentajes por cláusula de cumplimiento normativo
    c. Análisis de cumplimiento por cláusula, determinando los puntos críticos
2. Interpretación de los resultados obtenidos de la aplicación de la Guía técnica encuesta diagnóstico Modelo de Seguridad de la Información para las entidades del Estado propuesta por el MINTIC, mediante el uso de Microsoft Excel, para determinar el grado de madurez del SGSI.
3. Análisis de los resultados generales arrojados por ambos instrumentos

Fase 2: Análisis de riesgos

Esta fase permitió determinar catálogo de activos tipo, identificación de los escenarios de riesgos, que son la base para determinar los controles necesarios para cada escenario.

Fase 3: Selección de controles

Se generó declaración de aplicabilidad arrojada por el análisis de riesgo, luego de analizar el impacto de los controles seleccionados para cada uno de los escenarios de riesgo inherente

Fase 4: Diseño del modelo

En esta fase se construyó un esquema que permitió visualizar los requerimientos normativos del MINTIC, en contraste con los del MINEDUCACION, de tal manera que se pudiera plantear una alineación con los controles y requisitos de la Norma ISO 27001.

Esto permitió describir los pasos para la implementación de un SGSI que cumpla adecuadamente con las normativas antes mencionadas, en el área de Secretaria Académica de las instituciones públicas de educación de nivel básico.

Fase 5: Selección de herramienta de consulta para el Modelo del SGSI

Se realizó análisis de las características de cada una de las herramientas consultadas de tal manera que fuera posible determinar la que más se adecuara a las necesidades del modelo propuesto.

Fase 6: Validación y socialización del modelo

Se identifica el grado de aplicación del modelo, mediante la identificación de riesgos en los sujetos de validación.

2.1.6. Cuadro de resultados y/o productos esperados y potenciales beneficiarios

Tabla 3. Cuadro de resultados y/o productos esperados y potenciales beneficiarios.

Fuente: Propia

Aspecto	Resultado / Producto	Indicador	Beneficiario
Generación de nuevo conocimiento	Modelo de Gestión y Seguridad de la información	1 Modelo propuesto	Estrategia de Gobierno en Línea
Fortalecimiento de la comunidad Científica	Identificación de la alineación de los requisitos de la estrategia de GEL con el marco normativo de MEN	% de acoplamiento de la estrategia de GEL con la normatividad de MEN dada por la cantidad de requisitos normativos MEN cubiertos por la estrategia/Total de requisitos	Talento Digital Estrategia de Gobierno en Línea IED Secretarías de Educación
	Identificación de las brechas de cumplimiento normativo de las IED de nivel básico de carácter público respecto de la Norma ISO 27001:2013	1 Informe general de brechas de cumplimiento normativo	Estrategia de Gobierno en Línea IED Secretarías de Educación
	Identificación de los grados de madurez de los SGSI en las IED de nivel básico de carácter público de la comuna Universidad de la Ciudad de Pereira	1 Informe del grado de madurez de los SGSI en las IED	Estrategia de Gobierno en Línea IED Secretarías de Educación
	Identificación de los escenarios de riesgos de las IED de nivel básico de carácter público en términos de Seguridad de la Información	1 Informe de matrices de riesgos	Estrategia de Gobierno en Línea IED Secretarías de Educación
	Artículo para revista indexada con los resultados del proyecto	1 Artículo en proceso de publicación	Autores Comunidad Académica Talento Digital

Aspecto	Resultado / Producto	Indicador	Beneficiario
Apropiación social del conocimiento	Artículo para revista indexada con los resultados del proyecto	1 Artículo en proceso de publicación	Autores Comunidad Académica Talento Digital

2.1.7. Cuadro de impactos esperados

Tabla 4.Cuadro de impactos esperados.

Fuente: Propia

Impacto esperado	Plazo (años)*	Indicador verificable	Supuestos
Reducción de las brechas de cumplimiento normativo referentes a la Norma ISO 27001: 2013 en las IED´s	1	Porcentaje de cumplimiento normativo (ISO 27001:2013)	La IED implementará el modelo propuesto y lo mantendrá en el tiempo
Concientización de las IED´s en cuanto a la necesidad de implementar controles de seguridad de la información	4	Grado de madurez del SGSI	La IED implementará el modelo propuesto y lo mantendrá en el tiempo
Fortalecimiento de la información disponible acerca de la implementación de un SGSI en instituciones educativas de Nivel básico de carácter público.	2	1 Artículo publicado	La editorial a la cual se presenta el artículo acepta su publicación

2.2.Presupuesto

2.2.1. Global

Tabla 5. Presupuesto global del proyecto.

Fuente: Propia

PRESUPUESTO GLOBAL	
RUBROS	**TOTAL**
1. Gastos de personal	$49.280.000
2. Gastos de viaje	$780.000
3. Inversiones	$3.432.000
4. Servicios técnicos	$100.000
5. Gastos generales	$64.400
TOTAL	**$53.656.400**

2.2.2. Discriminado

Tabla 6. Presupuesto Gastos de Personal.

Fuente: Propia

1. GASTOS DE PERSONAL						
NOMBRE DEL PARTICIPANTE	**NIVEL DE FORMACIÓN**	**ROL EN EL PROYECTO**	**HORAS SEMANALES DEDICADAS AL PROYECTO**	**N° DE MESES**	**VALOR / HORA**	**TOTAL**
Alejandra Benavides	Especialista	Investigador	16	7	$35.000	$15.680.000
Carlos Blandón	Especialista	Investigador	16	7	$35.000	$15.680.000
Francisco Javier Valencia Duque	Doctorado	Asesor	8	7	$80.000	$17.920.000
			TOTAL GASTOS DE PERSONAL			**$49.280.000**

Tabla 7. Presupuesto gastos de viaje.

Fuente: Propia

2. GASTOS DE VIAJE							
ORIGEN	**DESTINO**	**TRAYECTO**	**N° DÍAS**	**N° DE PERSONAS**	**VALOR PERSONA**	**JUSTIFICACION**	**TOTAL**
Manizales	Pereira	Ida y regreso	12	1	$35. 000	Desplazamiento Alejandra María Benavides	420.000
Centro	IED's Comuna Universidad	Ida y regreso	12	8	$12.000	Recolección de Información, Entrega de informe	$288.000
Centro	IED Comuna San Fernando	Ida y regreso	3	2	$12.000	Recolección de Información, Entrega de informe	$72.000
TOTAL GASTOS DE VIAJE							**$780.000**

Tabla 8. Presupuesto inversiones.

Fuente: Propia

3. INVERSIONES				
DESCRIPCIÓN DEL EQUIPO	**CANTIDAD**	**VALOR UNITARIO**	**JUSTIFICACIÓN**	**TOTAL**
Portátil	2	$1.500.000	Para la elaboración del proyecto	$3.000.000
Impresora	1	$300.000	Impresión de documentación	$300.000
Cartuchos	2	$50.000	Tinta para la impresora	$100.000
Memoria USB	2	$16.000	Copias de seguridad de la documentación del proyecto y transporte de la documentación	$32.000
			TOTAL INVERSIONES	**$3.432.000**

Tabla 9. Presupuesto servicios técnicos.

Fuente: Propia

4. SERVICIOS TÉCNICOS				
DESCRIPCIÓN DEL SERVICIO TÉCNICO	**CANTIDAD**	**VALOR UNITARIO**	**JUSTIFICACIÓN**	**TOTAL**
Internet de 5 MB	2	$ 50.000	Consultas	$100.000
			TOTAL SERVICIOS TÉCNICOS	$100.000

Tabla 10. Presupuesto gastos generales.

Fuente: Propia

5. GASTOS GENERALES				
DESCRIPCIÓN DEL ARTÍCULO	**CANTIDAD**	**VALOR UNITARIO**	**JUSTIFICACIÓN**	**TOTAL**
Lapiceros	4	$800	Escribir anotaciones	$3.200
Cuadernillo	2	$1.000	Anotaciones	$2.000
Cosedora	1	$5.000	Coser los documentos	$5.000
Lápices	4	$700	Escribir anotaciones	$2.800
Borradores	4	$300	Para borrar	$1.200
Minas	4	$1200	Sacar punta a los lápices	$4.800
Encuadernación	1	$25.000	Encuadernar el informe Final	$25.000
Resma de papel	2	$10.200	Impresiones	$20.400
			TOTAL GASTOS GENERALES	$64.400

3. Referente teórico

3.1.Información

Las organizaciones han manejado a través de diversos mecanismos de almacenamiento información sobre las actividades realizadas tanto en el interior como en el exterior de la misma, dicho registro ha sido elemento esencial para la operatividad eficiente de los procesos organizacionales, la trazabilidad y elementos probatorios para dirimir conflictos y no conformidades de las partes interesadas en el negocio; en un mundo globalizado, donde la tecnología ha incursionado en todos los sectores productivos, encontramos una gran flexibilización de los mecanismos y herramientas que permiten el acceso global a esa información trayendo consigo riesgos, que ponen en peligro las dinámicas empresariales.

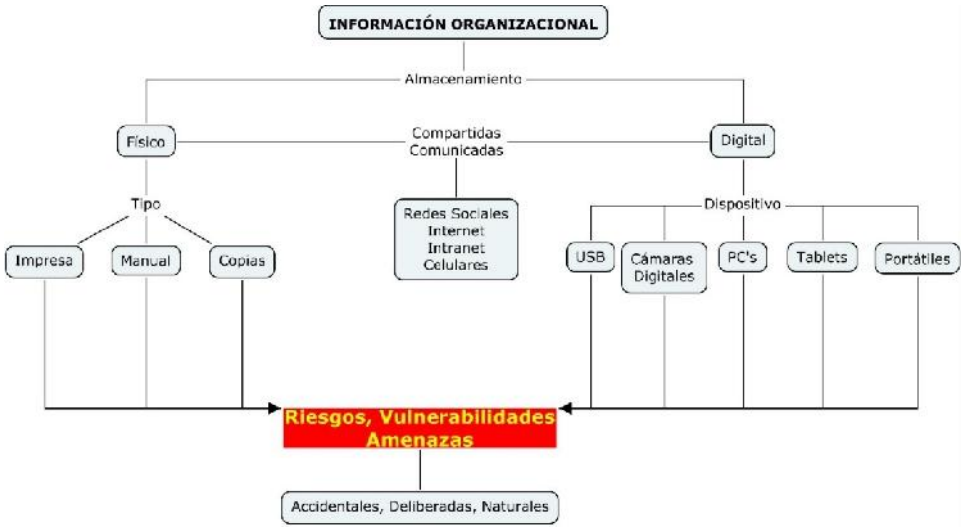
Como lo decía Sebastiá Salat Monserrat “Estamos creando redes sociales, estándares, etiquetas y metadatos, motores de búsqueda, archivos y bibliotecas digitales, portales temáticos, y sistemas de información de calidad (pasarelas temáticas) que sugieren la globalización de la información a la audiencia digital”, (Monserrat, 2008, pág. 23).

Como puede apreciarse en la gráfica 5, el hecho que la información se encuentre cada vez más digitalizada no implica que no se conserven aún registros en medio físico, clasificando entonces la información de acuerdo al medio de almacenamiento en:

1. Información digital
2. Información impresa

Las organizaciones deben entonces prepararse para una era de fácil acceso a las comunicaciones, donde los controles implementados para salvaguardar dicha información,

independiente del tipo de almacenamiento en el que se encuentre, pueden hacer la diferencia competitiva en un mundo globalizado y veloz que exige inmediatez en la consulta de información empresarial, y que a la vez representa un riesgo si es utilizado deliberadamente o accidentalmente de manera indebida.



Gráfica 5. Almacenamiento de Información Organizacional.

Fuente: Propia

3.2. Seguridad de la información

La Norma NTC ISO/IEC 27001:2013 la define como: preservación de la confidencialidad, integridad y disponibilidad de información (ISO, 2014), pero a la vez aclara que dicha seguridad puede involucrar características tales como la autenticidad, no repudio y fiabilidad.

Autenticidad: Propiedad de que una entidad es lo que dice ser (ISO, 2014).

No repudio: Capacidad que se tiene de probar la ocurrencia de un evento o acción que se atribuye y las entidades que lo originan (ISO, 2014).

Fiabilidad: Propiedad de tener un comportamiento y resultados previstos. (ISO, 2014)

La seguridad de la información, permite que las organizaciones aseguren la continuidad del negocio, gestionando sistemáticamente los riesgos e implementando adecuadamente controles que le permitan fortalecer su operatividad y competitividad, y a su vez contribuye a la toma de conciencia de los colaboradores de la misma en la importancia del empleo de buenas prácticas.

Dicha seguridad contempla la catalogación de los activos de información, identificación de escenarios de riesgos e implementación de controles de seguridad de la información

3.2.1. **Activo de información**

La información tiene un valor esencial para el funcionamiento de la organización, puesto que garantiza la trazabilidad, efectividad y eficiencia de las operaciones, así como el cumplimiento de las regulaciones gubernamentales, además permite aportar evidencia de cumplimiento a los entes de control, convirtiéndose con el pasar del tiempo en elemento importante de conocimiento de hechos pasados y abordados por la organización, garantizando la toma de decisiones basados en hechos y con información suficiente.

La Norma NTC ISO/IEC 27000 define: La información es un activo que, al igual que otros activos comerciales importantes es esencial para el negocio de una organización y por lo tanto necesita ser protegido de forma adecuada (ISO, 2014).

3.2.2. **Riesgo**

Se define de diferentes maneras por organizaciones como: la Real Academia de la Lengua, la norma internacional ISO/IEC 31000, el marco de gestión de riesgos COSO ERM, COBIT, tal como se aprecia en la gráfica 6

Gráfica 6. Definiciones de riesgo.

Fuente: propia

Convergen entonces las anteriores definiciones en la ocurrencia del daño a la organización como consecuencia de un evento, del cual se desconoce a ciencia cierta el día y hora en que se materializa el daño previsto.

Dichos riesgos pueden afectar los activos de la organización (humanos, lógicos, tecnológicos, físicos, etc.), los cuales pueden o no emplear en su quehacer cotidiano sistemas de información.

Para poder brindar una estimación cuantitativa del riesgo analizado es necesario identificar la probabilidad de ocurrencia, multiplicado por el impacto generado por la ocurrencia en sí mismo del riesgo.

$$N \quad d \quad v \qquad = (P \; x \; I) \qquad)/M \quad (P \; x \; I) \qquad)$$

Donde:

Cuantificación del Riesgo: Valor generado por el riesgo y que es determinante para evaluar si se acepta, se transfiere, se mitiga o se elimina.

P = Probabilidad de ocurrencia del riesgo.

Impacto = Daño generado por la ocurrencia del riesgo, teniendo en cuenta los tres criterios de la seguridad de la información: confidencialidad, integridad y disponibilidad.

Con los resultados generados durante la cuantificación del riesgo, empleando para ello la metodología más adecuada para la organización, se procede a diseñar el plan de mitigación de riesgos, que permitirá proteger los activos críticos que se encuentran en riesgo.

3.3. Sistemas de gestión de seguridad de la información

Teniendo claro que las organizaciones en el contexto actual, no solo generan, conservan, administran y requieren información física y digital para el correcto desarrollo de sus actividades de producción y comunicación y, que a su vez los mecanismos empleados para realizar las diversas transacciones con la información se han diversificado, generando la sensación de ubicuidad, al permitir el acceso remoto a la misma a través de dispositivos y redes de comunicaciones, abriendo de esta manera la probabilidad de ocurrencia de riesgos cada vez con mayor diversidad, cantidad e impacto a la organización, se requiere establecer metodologías y modelos que permitan garantizar el cuidado, la confidencialidad, integridad y disponibilidad de aquellos activos de información críticos para la operación de la empresa.

Aliaga Flores, define Sistema de Gestión de Seguridad de la Información como “Parte del sistema de gestión general, basada en un enfoque de riesgo comercial para establecer, operar, monitorear, revisar y mejorar la seguridad de la información”, (Aliaga Florez, 2013, pág. 22).

La Norma NTC ISO/IEC 27001, lo define como:

Es una parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, mantener y mejorar la seguridad de la información, permitiendo el control sobre los sistemas de información y la información que se maneja en la organización, (Instituto colombiano de normas técnicas y certificación, 2013)

3.4. Seguridad de la información y seguridad informática

Seguridad de la información

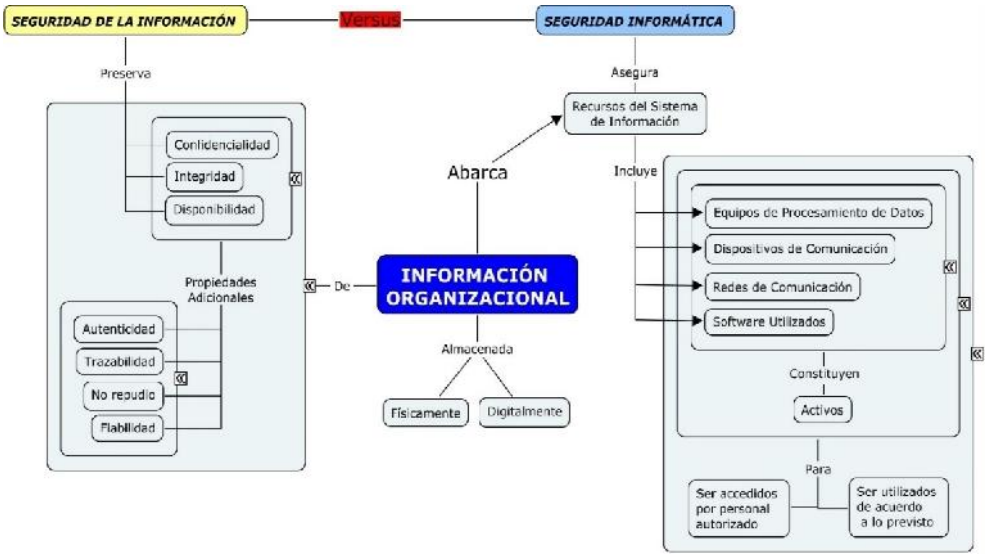
De acuerdo a la norma internacional ISO/IEC 27001:2013 “Está definida como la preservación de la confidencialidad, la integridad y la disponibilidad de la información, además, puede involucrar otras propiedades tales como autenticidad, trazabilidad, no repudio y fiabilidad”. (Instituto colombiano de normas técnicas y certificación, 2013, pág. 4)

Seguridad Informática

“Consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización”. (Torres Bermúdez, 2010, pág. 37).

A partir de lo establecido previamente, se concluye que la seguridad de la información involucra de manera inherente una identificación de activos críticos que generan, administran, conservan y comunican información en la organización tanto interna como externa, de acuerdo

con la definición dada por la norma NTC ISO/IEC 27001, lo que nos permite concluir en relación con lo expuesto por Torres Bermúdez, que la seguridad de la información involucra la seguridad informática, tal como se aprecia en la gráfica 7, incluyendo la implementación de controles al personal y los activos de tal manera que se garantice la confidencialidad, integridad y disponibilidad de la información.



Gráfica 7. Seguridad de información versus Seguridad informática.

Fuente: Propia

3.5. Criterios de seguridad de la información

La Norma NTC ISO/IEC 27001, y la Norma ISO 27000 hacen referencia a tres propiedades fundamentales para la seguridad de la información, ver gráfica 8:

1. Confidencialidad: “Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados”. (ISO, 2014, pág. 8)

2. Integridad: “Propiedad de la información relativa a su exactitud y completitud. Implica la protección de la información contra modificación o eliminación sin autorización”. (ISO, 2014, pág. 11)
3. Disponibilidad: “Propiedad de la información de estar accesible y utilizable cuando lo requiera la entidad”. (ISO, 2014, pág. 8)

Gráfica 8. Propiedades de la seguridad de la información.

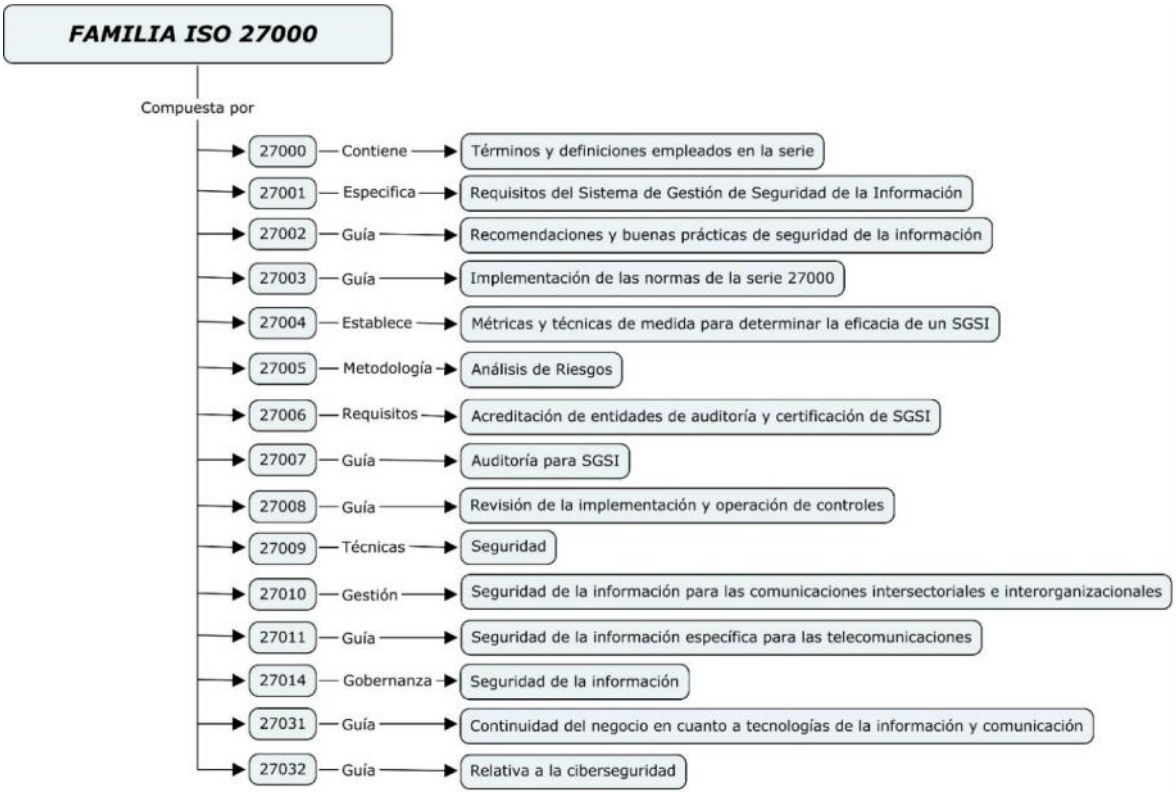
Fuente propia

3.6. Familia de Normas ISO/IEC 27000

La evolución de la familia Norma ISO/IEC 27000 data desde 1995, año en el cual la British Standards Institute, publica el primer conjunto de buenas prácticas conformado por las normas BS

7799-1 y BS 7799-2, que constituyen la guía de buenas prácticas y los requisitos para un sistema de seguridad de información respectivamente.

A partir 1999, momento en el que la Organización Internacional de Estándares, promueven la adopción de estándares a nivel mundial que procuran la competitividad de los diversos sectores económicos hace revisión de la BS 7799-1 y publica la norma ISO 17799.



Gráfica 9.Familia de normas ISO 27000.

Fuente: Propia

La primera publicación de la Norma ISO 27001 se llevó a cabo en el año 2005, y se cambió la denominación de la ISO 17799 a ISO 27002, la familia ISO 27000 ha crecido conforme a las necesidades generadas por los cambios en las dinámicas del mercado, del contexto, la

competitividad y los avances tecnológicos, creando una serie completa de normas que pertenecen a esta familia, las cuales se relacionan en la gráfica 9.

3.7. Normas a utilizar

3.7.1. ISO/IEC 27001

Describe los requisitos para el "el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información". (Instituto colombiano de normas técnicas y certificación, 2013, pág. 7). Como puede apreciarse en la gráfica 10, se basa en el ciclo PHVA, con enfoque en procesos, y su campo de aplicación abarca "todas las organizaciones, independientes de su tipo, tamaño o naturaleza", (Instituto colombiano de normas técnicas y certificación, 2013, pág. 8).

Gráfica 10. Circulo de Deming aplicado al SGSI,

Fuente: Elaborado a partir de NTC ISO/IEC 27001

Los requisitos exigidos por la norma para la implementación del Sistema de Gestión de Seguridad de la información se pueden dividir en varias etapas, las cuales se ilustran en la gráfica 11.

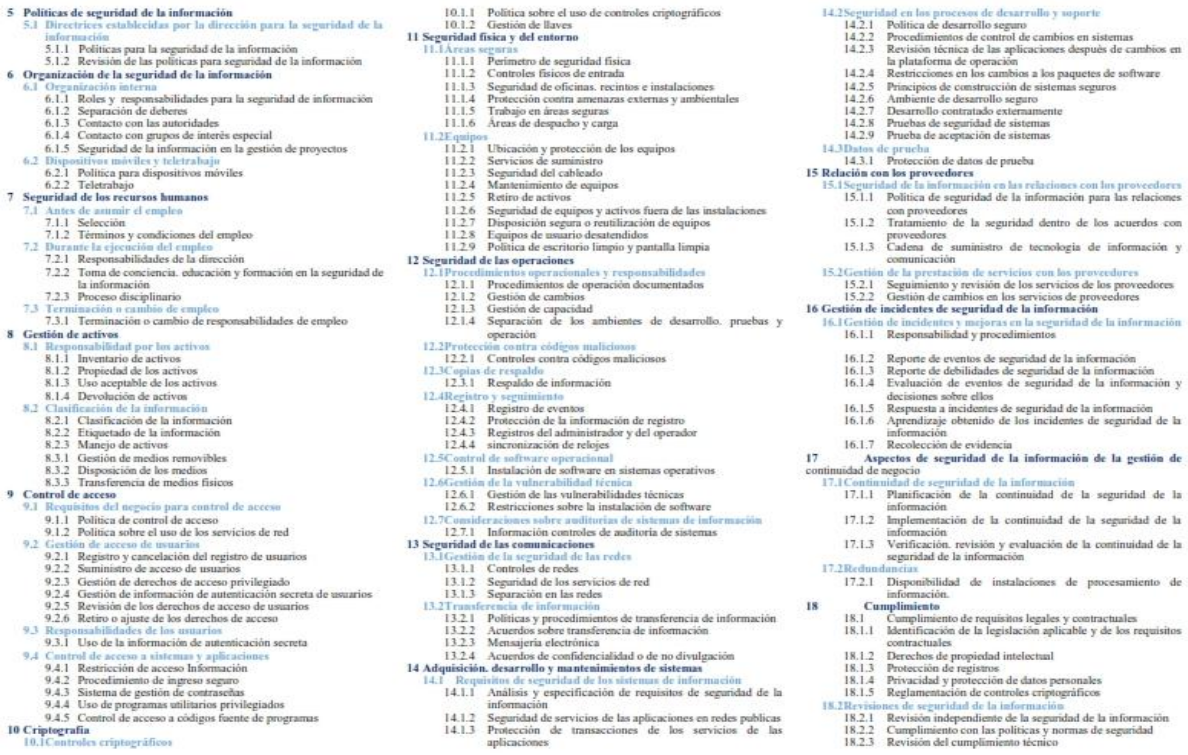
Gráfica 11. Sistemas de gestión de seguridad de la información.

Fuente: Propia

Siendo una norma aceptada internacionalmente y adoptada por el Ministerio de Tecnologías de la Información y las Comunicaciones, constituye de manera conjunta con la guía del MINTIC el principal marco referencial para la Implementación de los Sistemas de Gestión de Seguridad de la Información en las instituciones públicas del orden nacional y territorial obligadas por el Decreto 1078 de 2015.

3.7.2. **ISO/IEC 27002**

Esta norma, “contiene una lista de controles para la gestión de la seguridad de la información, por lo tanto, será el marco de referencia sobre la cual se establecerá la declaración de aplicabilidad”, (León Zuluaga & Grajales Valencia , 2016, pág. 44), ver gráfica 12.

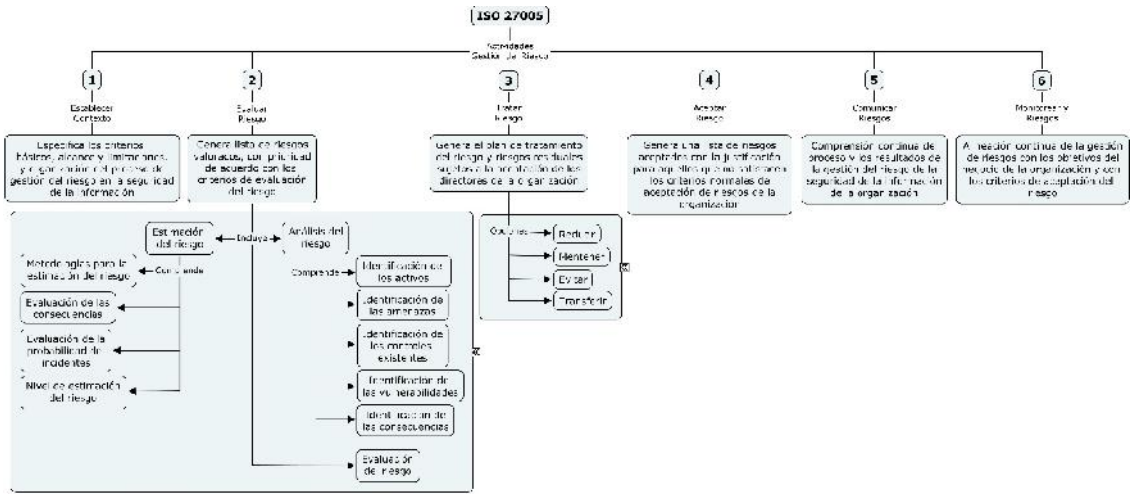


Gráfica 12. Controles establecidos en norma ISO 27002.

Fuente: (ISO27000.es, 2017)

3.7.3. **ISO/IEC 27005**

Proporciona directrices para la gestión de riesgos de seguridad de la información, dando soporte a los requisitos establecidos por la Norma NTC ISO/IEC 27001, se desarrolla a través de un conjunto de actividades, ilustradas en la gráfica 13, que permiten la gestión del riesgo en la seguridad de la información.



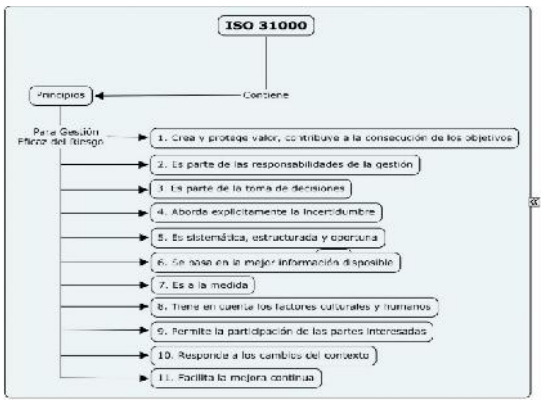
Gráfica 13. Actividades para la gestión del riesgo de acuerdo a ISO 27005

Fuente: propia

3.7.4. **ISO/IEC 31000**

Describe los principios y directrices para la gestión del riesgo, y lo define como “El efecto de incertidumbre en la consecución de los objetivos”, (ISO, 2009, pág. 4).

En la gráfica 14, se describen los principios para lograr una gestión eficaz del riesgo.



Gráfica 14. Principios Norma ISO 31000.

Fuente: Propia

Su implementación apoya el cumplimiento de la política y los objetivos de la organización.

3.8.Metodologías de riesgos

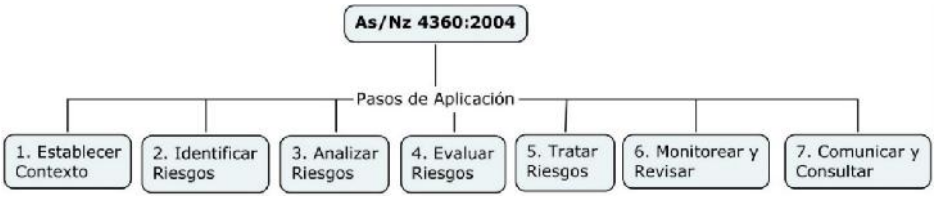
3.8.1. Norma Australiana As/Nz 4360:2004

Es una guía que apoya la implementación del proceso de la administración de riesgos dentro de la cual se determina el contexto y se realiza la identificación, análisis, evaluación, tratamiento, comunicación y monitoreo de los riesgos a los cuales está expuesta la organización.

Los principales objetivos en los cuales se enfoca AS/NZ 4360:2004 son, (AS/NZS, 1999):

1. Generar efectivamente la identificación de amenazas y sus vulnerabilidades en la ocurrencia.
2. Administrar rigurosamente los riesgos que permitan una oportuna toma de decisiones y la planificación y ejecución de proyectos.
3. Gestionar proactivamente frente a los riesgos y minimizar las reacciones reactivas frente a los mismos.
4. Garantizar con la correcta utilización de esta guía la reducción de pérdidas y el costo de los riesgos generados los cuales amenazan al cumplimiento de la legislación actual para la seguridad de la información.

Los pasos de aplicación para la gestión de los riesgos, (AS/NZS, 1999), se aprecian en la gráfica 15:



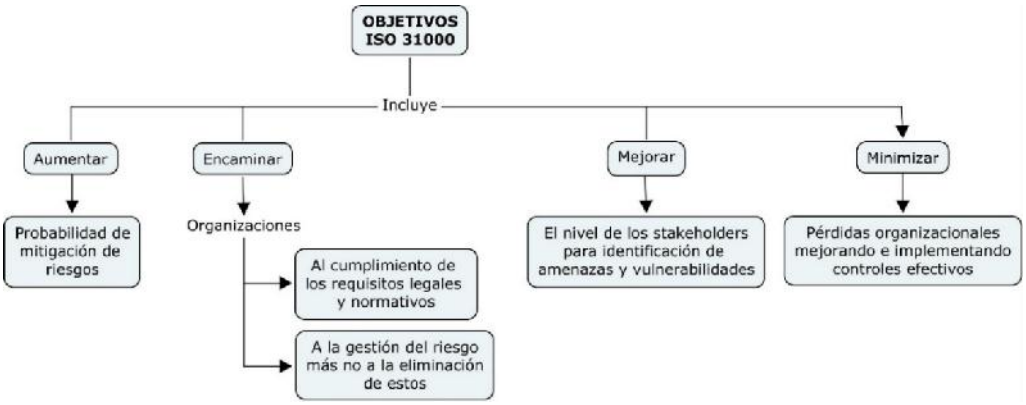
Gráfica 15. Pasos de aplicación para la gestión de riesgos Norma As/Nzs.

Fuente: Propia

3.8.2. **ISO 31000**

Establece los principios y directrices para la Gestión de Riesgos en las organizaciones, proporcionando además una guía para los programas de auditorías, (ISO, 2009).

La gráfica 16, presenta los principales objetivos de la norma.

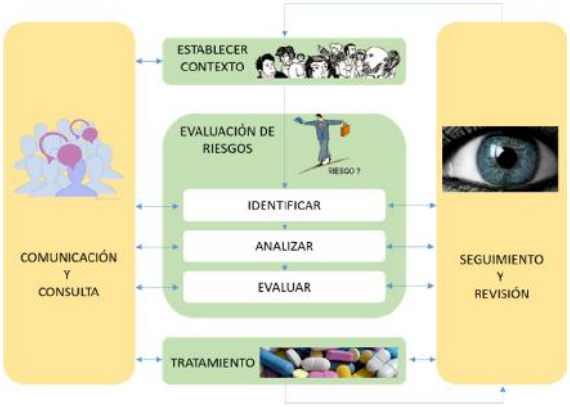


Gráfica 16. Objetivos ISO 31000:2009,

Fuente: Propia

La ISO 31000, establece una serie de etapas a seguir para lograr realizar una adecuada gestión del riesgo, las cuales se muestran en la gráfica 17, dentro de las cuales se encuentran la

comunicación y la consulta, el establecimiento del contexto de la organización, la evaluación de riesgos, el tratamiento, seguimiento y medición.



Gráfica 17 Proceso de gestión del riesgo

Adaptado de la Norma ISO 31000.

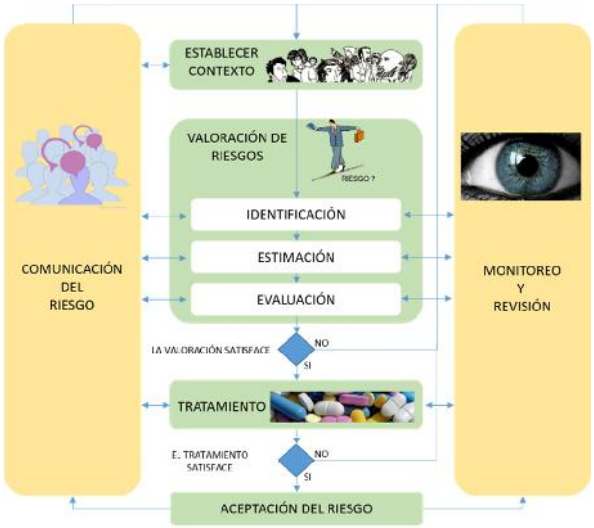
3.8.3. **ISO 27005**

Define una metodología para abordar la gestión de riesgos de la seguridad de la información constituyéndose en un marco de referencia; es aplicable a los sistemas de información de todas las organizaciones, por lo tanto, “se adapta al enfoque de gestión de riesgos de cualquiera de estas”, (Ramírez Castro & Ortiz Bayona, 2011, pág. 54).

El proceso de gestión de riesgos de seguridad de la información descrito por la norma se compone de varias fases y etapas, tal como puede observarse en las gráficas 18 y 19 respectivamente.

Gráfica 18. Fases ISO 27005.

Fuente: Propia



Gráfica 19. Mapa de Análisis de Riesgos bajo la norma ISO/IEC 27005.

Adaptado de (Ramírez Castro & Ortiz Bayona, 2011)

3.8.4. **Magerit versión 3**

Nace como iniciativa del Consejo Superior de Informática del Gobierno de España para dar respuesta a lo establecido en el "Decreto 3/2010 del 8 de enero, por él se regula el Esquema Nacional de Seguridad en el ámbito de administración electrónica". (Ministerio de la Presidencia, 2010).

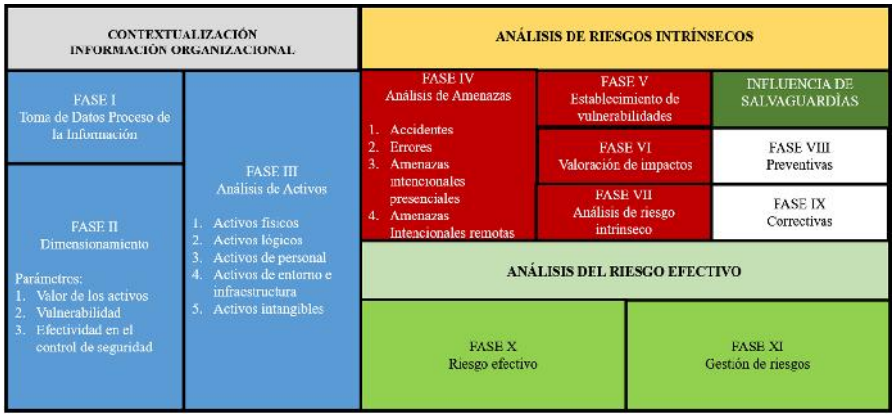
Magerit es conocida como la “Metodología para el Análisis y Gestión de Riesgos de los Sistemas de Información, utilizada para la mitigación y control de los riesgos a los cuales se enfrentan las organizaciones al momento de la implantación y uso de las TIC”, (Espinosa Betancur, García Gallo, & Giraldo Restrepo, 2016, pág. 38).

La metodología Magerit tiene como objetivo principal la incursión en las entidades de Administración Pública, propiciando y apoyando el cumplimiento de la normatividad de TIC del estado actual para beneficio de toda la ciudadanía, (Ministerio de hacienda y admnistraciones publicas, Gobierno de España, 2012)., los objetivos principales de la metodología se resumen en la gráfica 20.

Gráfica 20. Objetivos de Magerit V3.

Fuente: Propia

La gráfica 21 muestra las fases de ejecución para la Gestión de Riesgos de la metodología Magerit.



Gráfica 21. Fases Magerit Versión 3.

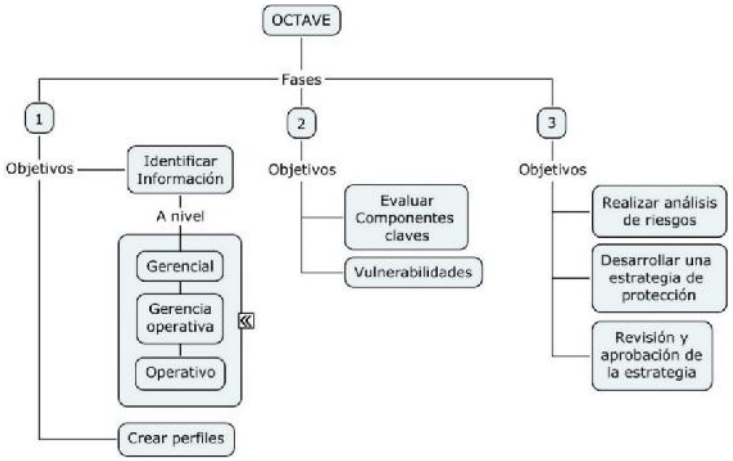
Fuente: Propia

3.8.5. **Operacionally critical threat, asset, and vulnerability evaluation (OCTAVE)**

Metodología desarrollada por el Software Engineering Institute, “las herramientas que pone a disposición para la gestión de riesgos tiene una alta complejidad, por lo que se aplica en entornos a gran escala”. (M. Talabis & L. Martín, 2013, pág. 3)

Esta metodología tiene tres versiones diferentes:

1. OCTAVE: Recomendada para gestión de riesgos en organizaciones que cuenten con más de 300 empleados, sus fases pueden observarse en la gráfica 22.



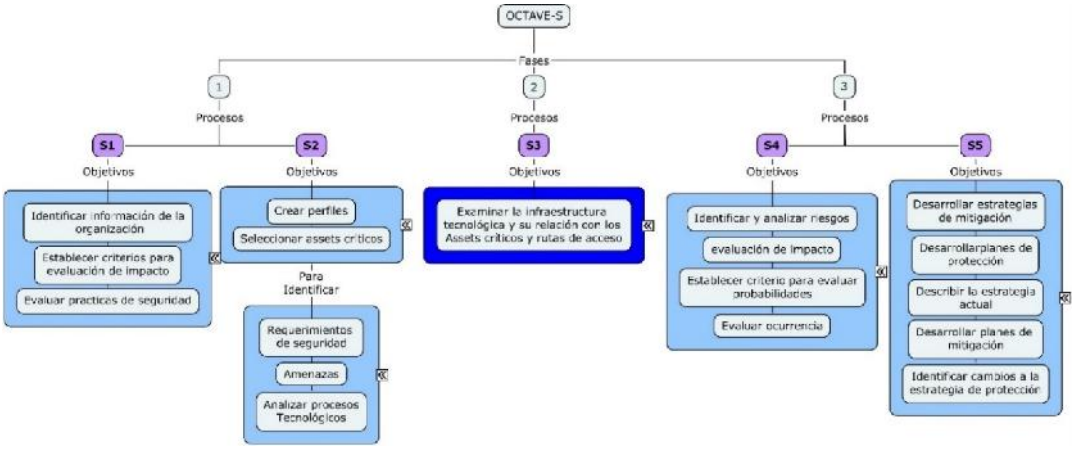
Gráfica 22. Fases de OCTAVE.

Fuente Propia

Como resultados esperados de las fases de OCTAVE se encuentran, (Muñoz, 2013):

1. Estrategia de protección: define el rumbo de la organización
2. Plan de mitigación: Diseñado para reducir el riesgo
3. Lista de acción: Acciones a corto plazo

2. OCTAVE – S: Versión para organizaciones con menos de 100 empleados, requiere de un equipo de 3 a 5 personas. Se divide en 3 fases (Muñoz, 2013, pág. 29), ilustradas en la gráfica 23.



Gráfica 23. Fases de OCTAVE- S.

Fuente: Propia

Como resultados esperados de las fases de OCTAVE – S se encuentran, (Muñoz, 2013, pág. 29):

1. Estrategia de protección: define el rumbo de la organización
2. Plan de mitigación: diseñado para reducir el riesgo
3. Lista de acción: acciones a corto plazo

3. OCTAVE – Allegro: Con características similares a la versión OCTAVE – S, para organizaciones pequeñas, pero sin una participación organizacional amplia, define las siguientes etapas:

   i. Definir criterios para la valoración del riesgo
   ii. Definir un perfil de activo de información
   iii. Identificar los contenedores de los activos de información
   iv. Identificar las áreas de interés

Como característica principal de la metodología está su diferencia de los análisis tradicionales enfocados a la tecnología, su flexibilidad y auto dirección. La gráfica 24, muestra las fases de la metodología.

Gráfica 24. Fases del proceso OCTAVE – Allegro

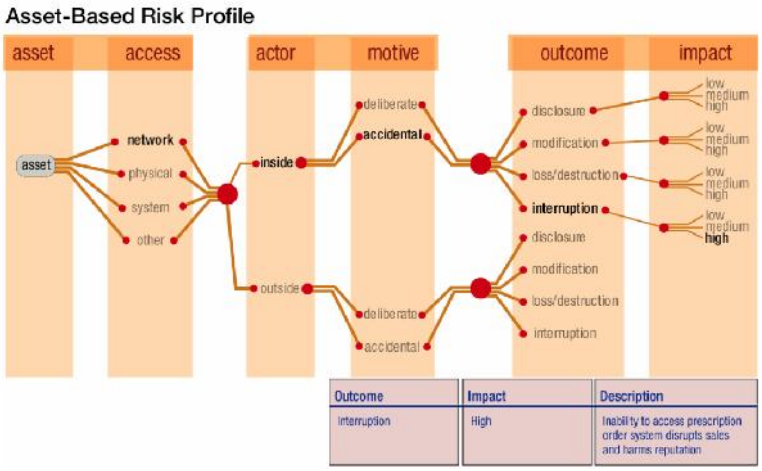
Adaptado de (Muñoz, 2013)

Dentro de las amenazas clasificadas por OCTAVE, ver gráfica 25, se encuentran:

1. Acciones humanas deliberadas
2. Acciones humanas accidentales
3. Problemas en los sistemas

Los que pueden desencadenar en consecuencias tales como:

4. Revelación de información crítica
5. Modificación de información crítica
6. Destrucción o pérdida de información crítica, hardware o software
7. Interrupción del acceso a información importante, aplicaciones o servicios



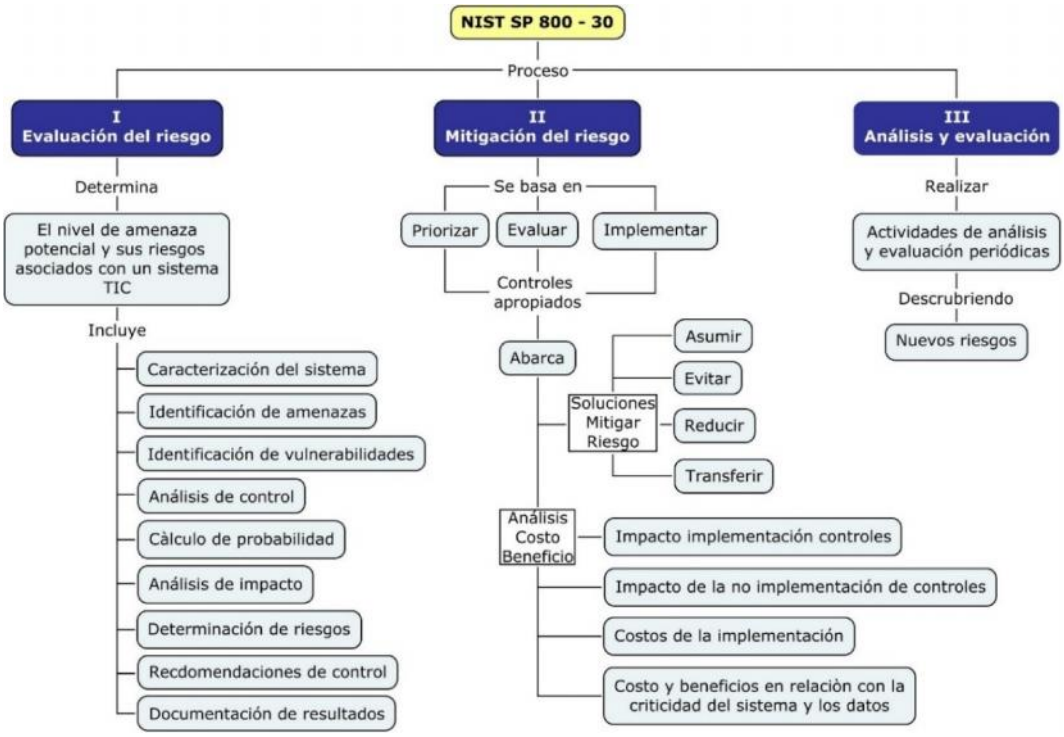
Gráfica 25. Perfil de riesgos basado en activos

Fuente: (Muñoz, 2013, pág. 15)

3.8.6. **NIST SP 800 – 30**

NIST SP 800-30, es una guía de Gestión de Riesgos de los Sistemas de Tecnología de la Información, se centra principalmente en la evaluación de riesgos que puede ser aplicada a cualquier tipo de organización pública o privada, así mismo abarca cualquier tipo de sector o industria.

La gráfica 26, presenta los tres pasos de la metodología del NIST SP 800-30 (Détienne, y otros, 2002).



Gráfica 26. Procesos NIST SP 800-30.

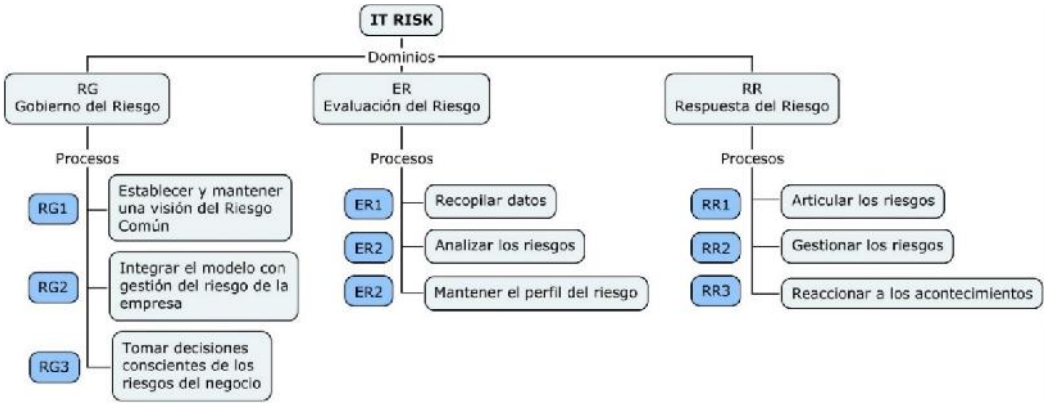
Fuente: Propia

3.8.7. **IT Risk de ISACA**

La metodología de riesgos planteada por la ISACA pretende evaluar todos los riesgos de TI importantes para la organización basándose en COBIT y Val IT, (Peña Ibarra, 2009). Risk IT es contiene un conjunto de principios, procesos de negocio y directrices para gestionar eficientemente los riesgos relacionados con las tecnologías de información. Este marco es complementario a COBIT pero se diferencia porque establece las mejores prácticas con el fin de establecer un marco para las organizaciones para identificar, gobernar y administrar los riesgos asociados a su negocio, (Caviedes Sanabria & Prado Urrego, 2012, pág. 83).

Puede ser empleada por todas las organizaciones que deseen establecer la dirección y seguimiento del riesgo a nivel de organización y los encargados de TI y de los departamentos de negocio que necesitan definir el proceso de la gestión de riesgos.

El modelo IT RISK se divide en 3 dominios, (Peña Ibarra, 2009, pág. 36), cada uno de los cuales tiene 3 procesos, detallados en la gráfica 27:



Gráfica 27. Dominios y procesos ITRISK – ISACA.

Fuente: Propia

3.8.8. **Metodología de riesgos de MINTIC**

El Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, puso a disposición de las entidades públicas del orden nacional y territorial, una guía que puede ser empleada como marco de referencia para la gestión de riesgos, la cual está basada en la norma Internacional ISO 27001. Este documento permite a las instituciones implementar buenas prácticas para el manejo de los riesgos integrándolo con la Metodología de Gestión de Riesgos del Departamento Administrativo de la Función Pública - DAFP.

(MINTIC, 2016), en su guía No. 7, sugiere las siguientes tres etapas para que cada entidad pueda administrar los riesgos realizando una serie de actividades de acuerdo a las necesidades de cada entidad.

La gráfica 28, presenta las actividades de gestión de riesgo propuestas por la guía del MINTIC.

ETAPAS DEL MSPI	PROCESO DE GESTION DEL RIESGO EN LA SEGURIDADDE LA INFORMACION
Planear	Establecer Contexto Valoración del Riesgo Planificación del Tratamiento del Riesgo Aceptación del Riesgo
Implementar	Implementación del Plan de Tratamiento de Riesgo
Gestionar	Monitoreo y Revisión Continuo de los Riesgos
Mejora Continua	Mantener y Mejorar el Proceso de Gestión del Riesgo en la Seguridad de la Información.

Gráfica 28 Etapas de la gestión del riesgo a lo largo del MSPI.

Fuente: (MINTIC, 2016)

Para el análisis de los riesgos se deben tener en cuenta las 7 etapas definidas en la Guía de gestión de riesgos, (MINTIC, 2016).

1. Identificación del riesgo: pretende identificar y caracterizar aquellos sucesos que generan incertidumbre en cuanto a su ocurrencia, que son previsibles y que tienen efectos negativos en la organización.
2. Identificación de los activos, “un activo es todo aquello que tiene valor para la entidad y que, por lo tanto, requiere de protección”, (MINTIC, 2016, pág. 19), consiste en determinar las consecuencias de la ocurrencia de un riesgo identificado en el activo analizado, de tal manera que sea factible valorarlo, para analizar su criticidad real.

3. Identificación de amenazas, permite identificar aquellos eventos naturales o personas que actúan de manera accidental o deliberada y que pueden ocasionar daños en uno o varios de los activos identificados en la etapa anterior.
4. Identificación de controles existentes, determinación de la planificación, operatividad y efectividad de los controles existentes.
5. Identificación de las vulnerabilidades, estas deben ser valoradas a través de métodos existentes, y para ello se deben conocer el inventario de activos, amenazas y los controles definidos.
6. Valoración de vulnerabilidades técnicas: identificación de las deficiencias en términos de seguridad que se encuentren relacionadas a los activos identificados, información o personas.

Identificación de consecuencias, “se deben identificar los daños o las consecuencias para entidad que podrían ser causadas por un escenario de incidente”, (MINTIC, 2016), lo que se traduce en la caracterización detalla de los problemas ocasionados por la ocurrencia del riesgo identificado.

3.9.La educación básica y la seguridad de la información

3.9.1. Contexto general de la educación básica

La educación es un derecho incluido en la declaración universal de los derechos humanos, (Comisión de derechos humanos, 1948), la convención por los derechos del niño, (UNICEF

Comité Español, 2006) y el pacto internacional de los derechos económicos, sociales y culturales, (Naciones Unidas, 1976), como puede verse en la gráfica 29.

Declaración universal de los derechos humanos, Arts. 25 y 26	Convención por los derechos del niño, Arts. 2, 6, 28, 32, 34	Pacto internacional de los derechos económicos, sociales y culturales, Arts 10, y 13
"Toda persona tiene derecho a un nivel de vida adecuado que le asegure, así como a su familia, la salud y el bienestar, y en especial la alimentación, el vestido, la vivienda, la asistencia médica y los servicios sociales necesarios.... Toda persona tiene derecho a la educación. La educación debe ser gratuita, al menos en lo concerniente a la instrucción elemental y fundamental. La instrucción elemental será obligatoria....."	*"Los Estados Partes respetarán los derechos enunciados en la presente Convención y asegurarán su aplicación a cada niño sujeto a su jurisdicción, sin distinción alguna ... todo niño tiene el derecho intrínseco a la vida... la supervivencia y el desarrollo del niño... Los Estados Partes reconocen el derecho del niño a la educación... Implantar la enseñanza primaria obligatoria y gratuita para todos... el derecho del niño a estar protegido contra la explotación económica y contra el desempeño de cualquier trabajo que pueda ser peligroso o entorpecer su educación... nocivo para su salud o para su desarrollo físico, mental, espiritual, moral o social. ... Los Estados Partes se comprometen a proteger al niño contra todas las formas de explotación y abusos sexuales..."*	*"Los Estados Partes en el presente Pacto reconocen que.... Se deben adoptar medidas especiales de protección y asistencia en favor de todos los niños y adolescentes, sin discriminación alguna ... Los Estados Partes en el presente Pacto reconocen el derecho de toda persona a la educación..... La enseñanza primaria debe ser obligatoria y asequible a todos gratuitamente...Los Estados Partes en el presente Pacto se comprometen a respetar la libertad de los padres y, en su caso, de los tutores legales, de escoger para sus hijos o pupilos escuelas distintas de las creadas por las autoridades públicas, siempre que aquéllas satisfagan las normas mínimas que el Estado prescriba o apruebe en materia de enseñanza..."*

Gráfica 29. Obligaciones de los gobiernos para asegurar los derechos de los niños y jóvenes.

Fuente: Propia

El Gobierno de Colombia incluye en la Carta Magna de 1991, las normas que reglamentan la educación, por cuanto es importante analizar la relación y puntos de convergencia normativa entre los requerimientos de seguridad de la información emanados por el MINTIC a través de la Estrategia de Gobierno en Línea, el MEN y los requisitos de la Norma Internacional ISO/IEC 27001.

El artículo 44 de la Constitución Política de Colombia de 1991, reza:

> Son derechos fundamentales de los niños: la vida, la integridad física, la salud y la seguridad social, la alimentación equilibrada, su nombre y nacionalidad, tener una familia y no ser separados de ella, el cuidado y amor, ***la educación*** y la cultura, la recreación y la libre expresión de su opinión. Serán protegidos contra toda forma de abandono, violencia

> física o moral, secuestro, venta, abuso sexual, explotación laboral o económica y trabajos riesgosos. Gozarán también de los demás derechos consagrados en la Constitución, en las leyes y en los tratados internacionales ratificados por Colombia... Art. 44, (Constitución Política de Colombia, 1991, pág. 24)

El artículo 67 de la Constitución Política de Colombia de 1991, indica: "El Estado, la sociedad y la familia son responsables de la educación, que será obligatoria entre los cinco y los quince años de edad y que comprenderá como mínimo, un año de preescolar y nueve de educación básica." Art. 67, (Constitución Política de Colombia, 1991, pág. 36)

Brindando convergencia y coherencia con los tratados internacionales, las exigencias del MINTIC a través de la Estrategia de Gobierno en Línea, el MEN y los requisitos de la Norma Internacional ISO/IEC 27001, el Art. 67 de la Constitución de 1991 establece que:

> Corresponde al estado regular y ejercer la suprema inspección y vigilancia de la educación con el fin de velar por su calidad, por el cumplimiento de sus fines y por la mejor formación moral, intelectual y física de los educandos; garantizar el adecuado cubrimiento del servicio y asegurar a los menores las condiciones necesarias para su acceso y permanencia en el sistema educativo, (Constitución Política de Colombia, 1991, pág. 36).

> El 8 de febrero de 1996, se expide la ley 115 – Ley General de Educación, la cual de conformidad con el artículo 67 de la Constitución Política en su artículo 1, define la educación formal en los niveles de preescolar, básica (Primaria y secundaria) y media, tal como sigue (León Zuluaga & Grajales Valencia , 2016):

> "Ley 115/1994 - Artículo 1**:** De conformidad con el artículo 67 de la Constitución Política, define y desarrolla la organización y la prestación de la educación formal en sus niveles preescolar, básica (primaria y secundaria) y media, no formal e informal, dirigida a niños

> y jóvenes en edad escolar, a adultos, a campesinos, a grupos étnicos, a personas con limitaciones físicas, sensoriales y psíquicas, con capacidades excepcionales, y a personas que requieren rehabilitación social." Art. 1, (Ley 115, 1994, pág. 1)
>
> La educación formal se organizará entonces en (3) niveles a saber:
>
> a) El preescolar que comprenderá mínimo un grado obligatorio;
>
> b) La educación básica con una duración de nueve (9) grados que se desarrollará en dos ciclos: La educación básica primaria de cinco (5) grados y la educación básica secundaria de cuatro (4) grados, y
>
> c) La educación media con una duración de dos (2) grados. Art. 11, (Ley 115, 1994, pág. 4)

La Ley General de Educación en su artículo 2 establece que el servicio educativo está conformado por los siguientes elementos:

> El conjunto de normas jurídicas, los programas curriculares, la educación por niveles y grados, la educación no formal, la educación informal, los establecimientos educativos, las instituciones sociales (estatales o privadas) con funciones educativas, culturales y recreativas, los recursos humanos, **tecnológicos,** metodológicos, materiales, administrativos y financieros, articulados en procesos y estructuras para alcanzar los objetivos de la educación. Art. 2, (Ley 115, 1994, pág. 1)

Lo que indica que la prestación de la función pública en torno al servicio educativo de nivel básico está conformada entre otros por elementos relacionados con los recursos tecnológicos que permiten la operación de las Instituciones Educativas, dando un punto de convergencia con las directrices emanadas por la norma ISO/IEC 27001.

La Ley 715/2001 define institución educativa en su artículo 9 así:

> Institución educativa es un conjunto de personas y bienes promovida por las autoridades públicas o por particulares, cuya finalidad será prestar un año de educación preescolar y nueve grados de educación básica como mínimo, y la media. Las que no ofrecen la totalidad de dichos grados se denominarán centros educativos y deberán asociarse con otras instituciones con el fin de ofrecer el ciclo de educación básica completa a los estudiantes. Art. 9, (Ley 715, 2001, pág. 6)

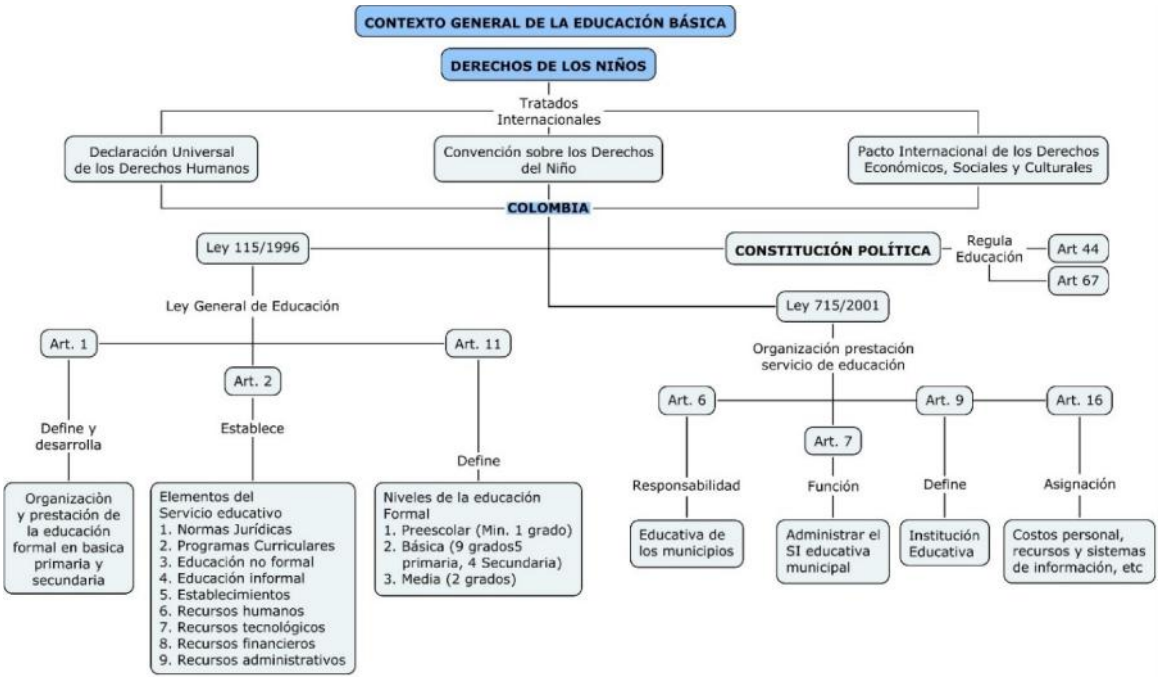
Se evidencia entonces que frente al servicio educativo los municipios tienen las siguientes responsabilidades:

"Dirigir, planificar; y prestar el servicio educativo en los niveles de preescolar, básica, media en sus distintas modalidades, en condiciones de equidad, eficiencia y calidad, en los términos definidos en la presente ley.". Art. 6, Numeral 6.2.1 (Ley 715, 2001, pág. 3), así mismo es función "Administrar el Sistema de Información Educativa Municipal o Distrital y suministrar la información al departamento y a la Nación con la calidad y en la oportunidad que señale el reglamento". Art. 7, Numeral 7.10 (Ley 715, 2001, pág. 5)

La población atendida por las instituciones educativas será asignada de acuerdo a las variables de la prestación del servicio educativo y dependiendo de la zona (rural o urbana), dentro de los cuales se encuentran (León Zuluaga & Grajales Valencia , 2016)

> ...los costos del personal docente y administrativo requerido en las instituciones educativas incluidos los prestacionales, los recursos destinados a calidad de la educación que corresponden principalmente a dotaciones escolares, mantenimiento y adecuación de infraestructura, cuota de administración departamental, interventoría y sistemas de información., Art. 16, Numeral 16.1.1 (Ley 715, 2001, pág. 9)

Podemos ver como en Colombia el contexto de educación, en este caso para nivel básica, se reglamenta por diferentes normativas nacionales y documentos expedidos y adoptados a nivel internacional, como se aprecia en la gráfica 30



Gráfica 30. Contexto general de la educación básica en Colombia.

Fuente: Propia

3.9.2. **Marco legal de la educación básica relacionada con la seguridad de la información**

Con el fin de garantizar transparencia y eficiencia en los procesos de las entidades del estado, el gobierno colombiano a través del Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC, ha expedido una serie de lineamientos relacionados en la Estrategia de Gobierno en Línea - GEL, para que mediante el uso de herramientas tecnológicas se acerque el

estado al ciudadano procurando garantizar la confidencialidad, disponibilidad e integridad de la información.

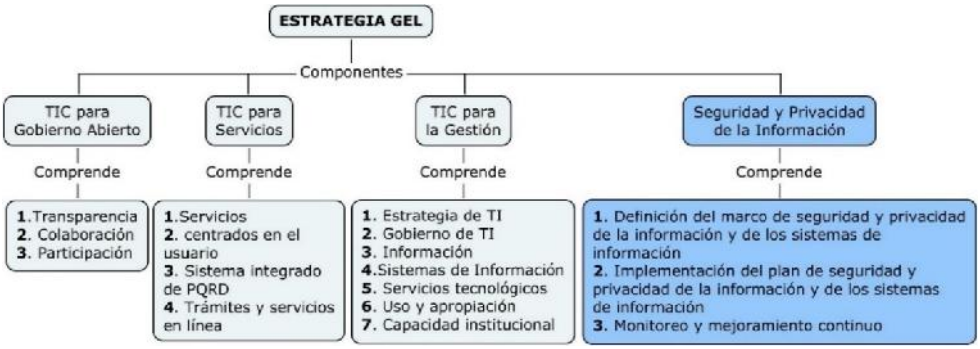
El Decreto 1078 del 26 de mayo de 2015**,** describe las directrices que todas las instituciones de carácter público deben seguir con el objetivo de acogerse a la Estrategia de GEL, implicando obligatoriedad para las instituciones educativas de carácter oficial que dan cobertura a la educación básica.

Dicho Decreto en el titulo 9 “Políticas y lineamientos de tecnologías de la información”, capítulo I “Estrategias de Gobierno en Línea”, da las indicaciones pertinentes para la construcción de un gobierno más “abierto, más eficiente, más transparente y más participativo y que preste mejores servicios con la colaboración de toda la sociedad”, Art, 2.2.9.1.1.1 (Decreto 1078, 2015, pág. 134).

Dicho Decreto es de obligatorio cumplimiento a “las entidades que conforman la administración pública” Titulo 9, Capitulo 1, Sección 1, Art, 2.2.9.1.1.2 (Decreto 1078, 2015, pág. 134), dentro de las cuales se encuentran “los ministerios, los departamentos administrativos y las superintendencias constituyen el sector central de la Administración Pública Nacional. Las gobernaciones, las alcaldías y las secretarías de despacho son los organismos principales de administración en el correspondiente nivel territorial”. Art, 39, (Ley 489, 1998, pág. 10)

La Estrategia de GEL se desarrollará conforme a los principios del debido proceso, igualdad, imparcialidad, buena fe, moralidad, participación, responsabilidad, transparencia, publicidad, coordinación, eficacia, economía y celeridad consagrados en los artículos 208 de la Constitución Política, 3° de la ley 489 de 1998 y 3° de la ley 1437 de 2011. Titulo 9, Capitulo 1, Sección 1, Art, 2.2.9.1.1.4 (Decreto 1078, 2015, pág. 135).

La gráfica 31 muestra los componentes de la Estrategia de GEL:



Gráfica 31. Componentes de GEL.

Fuente: Propia

Para lograr los objetivos de la estrategia GEL se ha puesto a disposición de las entidades públicas un Manual de Gobierno en Línea, el cual “define las acciones que corresponde ejecutar a las entidades del orden nacional y territorial respectivamente”, Titulo 9, Capitulo 1, Sección 2, Art, 2.2.9.1.2.2 (Decreto 1078, 2015, pág. 137), al igual que una guía para realizar el diagnóstico inicial para la implementación del Sistema de Gestión de Seguridad de la Información – SGSI.

El establecimiento del SGSI permite además dar cumplimiento a la política establecida en el documento CONPES 3854 de 2016, particularmente a los siguientes objetivos:

1. Establecer un marco institucional para la seguridad digital consistente en un enfoque de gestión de riesgos. (Departamento Nacional de Planeación, 2016)
2. Fortalecer la seguridad de los individuos y del estado en el entorno digital a nivel nacional y trasnacional, con un enfoque de gestión de riesgos. (Departamento Nacional de Planeación, 2016)

Con relación a los sistemas de información en la prestación del servicio de educación básica el Decreto 1526 de 2002 establece la reglamentación para la administración de los SI del sector educativo, el Art 1 determina “El sistema estará compuesto por información que permita realizar el monitoreo del servicio educativo y la evaluación de sus resultados”, (Presidencia de la Republica de Colombia, 2002, pág. 1), así mismo el Art. 4 brinda las características de calidad de la información y responsabilidad del tratamiento de las mismas al indicar:

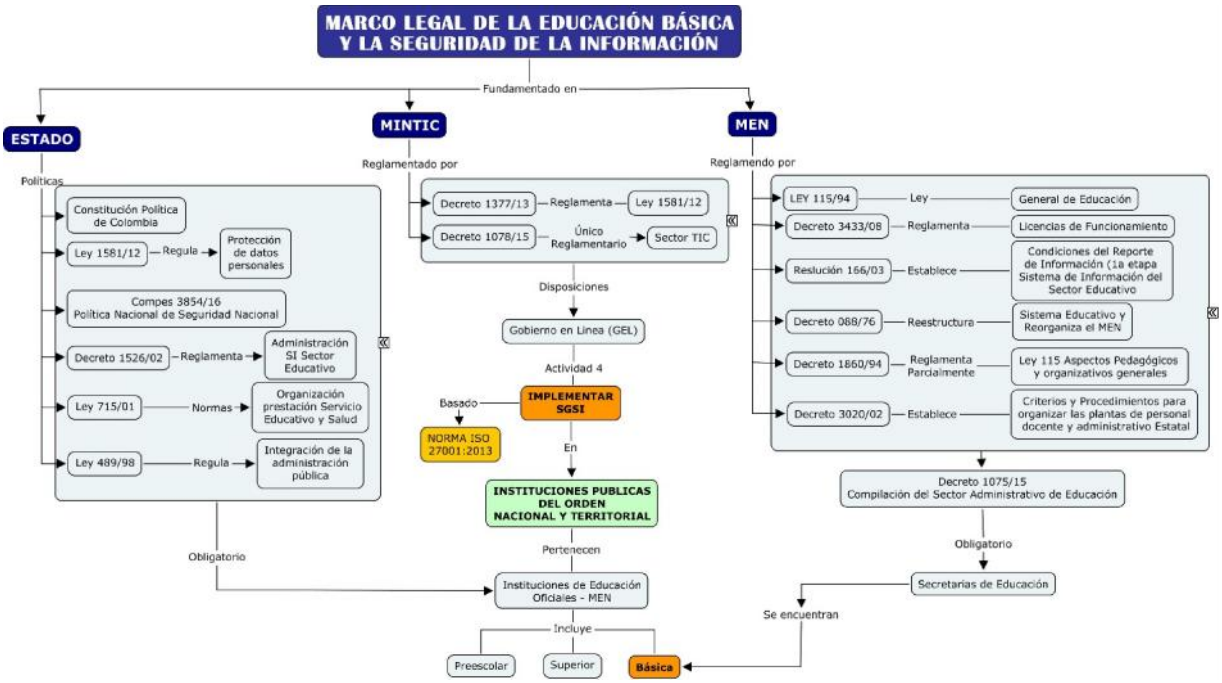
> …Para efectos de garantizar la calidad de la información, la Nación realizará periódicamente la validación y verificación de la información reportada por los departamentos, distritos y municipios certificado … será responsabilidad de cada entidad territorial, una vez al año, efectuar las auditorías que considere necesarias a la misma y la información de la población matriculada y del personal docente y administrativo y contrastarla con la información de la Registraduría Nacional del Estado Civil, (Presidencia de la Republica de Colombia, 2002, pág. 2).

En relación a los SI de las Instituciones Educativas la Ley 1581 de 2012, reglamentada parcialmente por el Decreto 1377 de 2013, en su artículo 7 establece:

> Es tarea del estado y de las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del tratamiento indebido de sus datos personales... Art, 7, (Ley 1581, 2012, pág. 4)

Lo anterior en coherencia con la Ley 715/2001 que contiene las disposiciones para organizar la prestación de los servicios de educación y salud, Titulo II, Capítulos 1 al 6, con la Ley 115/1994 Art. 2 Recursos tecnológicos y la Resolución 166/2003 que contiene las

condiciones para el reporte de información de las IED’s, recopiladas todas estas disposiciones en el Decreto único reglamentario del sector de educación 1075/2015, ver gráfica 32.



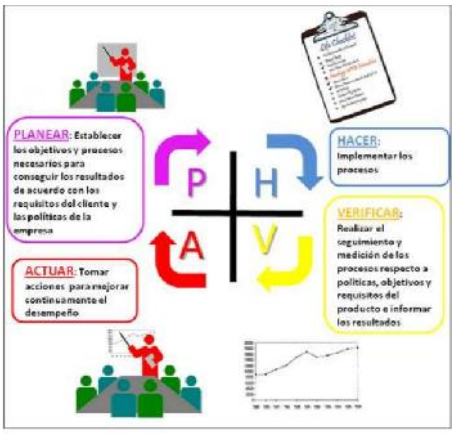
Gráfica 32 . Marco legal de la educación básica y la seguridad de la información en Colombia. Fuente Propia

3.9.3. Relevancia de la seguridad de la información en la prestación del servicio educativo de nivel básico

Beneficios de la implementación de un SGSI basado en ISO 27001:

1. Metodología de gestión de riesgos: permite identificar y priorizar amenazas y riesgos del contexto educativo, estableciendo controles que permitan aceptar, evitar, mitigar o transferir los riesgos, generando estabilidad, continuidad y confianza.

2. Mejora continua: basa su funcionamiento en la metodología del ciclo de Deming (P – Planear, H – Hacer, V – Verificar, A - Actuar), (NTC ISO/IEC 27001, 2013), para lo cual es necesario ejecutar ciclos de auditorías que permitan determinar la efectividad de los controles implementados, ver gráfica 33.



Gráfica 33: Ciclo de Deming.

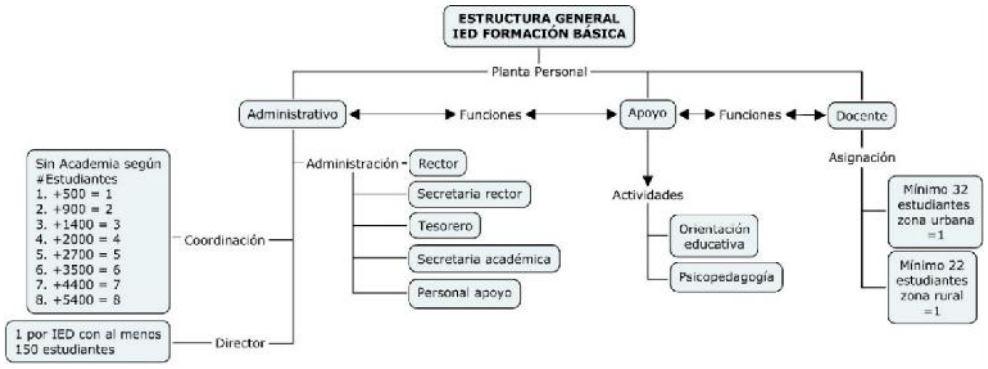
Fuente: (Buitrago Estrada, Bonilla Pineda, & Murillo Varón, 2012)

1. Disponibilidad del Servicio Educativo
2. Reducción de costos de incidentes e inversiones: permite establecer mecanismos de respuesta oportuna a la posible ocurrencia de los riesgos identificados, evitando detener la operación de los procesos organizacionales.
3. Cumplimiento de la legislación: Cierra las brechas de cumplimiento “entre lo exigido por el gobierno nacional a través de la Estrategia de Gobierno en Línea y asegura el cumplimiento del marco legal aplicable al sector educativo y al tratamiento de datos en general”, (León Zuluaga & Grajales Valencia , 2016).
4. Incremento de los niveles de confianza de los stakeholders.

5. Mejora de la imagen institucional
6. Establecimiento e identificación de responsabilidades caracterizando las actividades relacionadas con la seguridad de la información.

3.9.4. **Estructura docente y administrativa de las IED de nivel básico**

El Decreto 1075 de 2015 establece la estructura del sector educativo en cabeza del MEN por parte del Gobierno Nacional, secretarias de educación departamentales, secretarias de educación municipales, quienes velaran en su jurisdicción por el adecuado manejo del servicio educativo de todas las instituciones educativas, (León Zuluaga & Grajales Valencia , 2016), la gráfica 34 refleja de manera general la estructura organizacional.



Gráfica 34. Estructura general IED formación básica.

Fuente: Propia

4. Diagnóstico del sistema de gestión de seguridad de la información en los establecimientos educativos

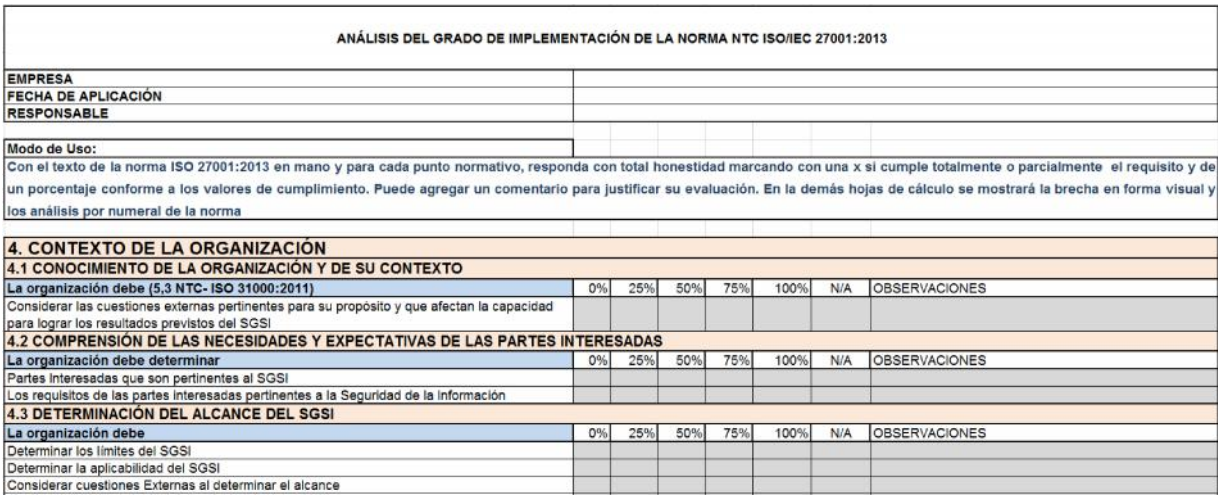
4.1. Diagnósticos iniciales de las IED

Para determinar el diagnóstico inicial de las IED's pertenecientes a la Comuna Universidad de la ciudad de Pereira – Risaralda en relación a las brechas de cumplimiento con los requisitos establecidos en la Norma Internacional NTC ISO/IEC 27001:2013 y diagnosticar el grado de madurez de los SGSI establecidos actualmente por cada una de ellas se aplicaron los siguientes instrumentos:

1. Herramienta para determinar las brechas de cumplimiento de requisitos de la Norma ISO 27001:2013, diseñada durante el desarrollo del trabajo.
2. Guía encuesta diagnóstico modelo de seguridad de la información para las entidades del estado, proporcionado por MINTIC.

4.1.1. Diagnóstico de brechas de cumplimiento de requisitos de la Norma NTC ISO/IEC 27001:2013

El instrumento presentado en la gráfica 35 se diseñó en Microsoft Excel versión 2016, permite realizar un análisis de los requisitos establecidos por la Norma internacional NTC ISO/IEC 27001:2013, ubicando aquellos que implican obligatoriedad de cumplimiento en la cláusula correspondiente, es decir aquellos que emplean la forma verbal Debe para su descripción no fueron incluidas las formas verbales Debería y Puede en razón a la interpretación de recomendación y permiso respectivamente por parte de la norma internacional.



ANÁLISIS DEL GRADO DE IMPLEMENTACIÓN DE LA NORMA NTC ISO/IEC 27001:2013							
EMPRESA							
FECHA DE APLICACIÓN							
RESPONSABLE							
Modo de Uso:							
Con el texto de la norma ISO 27001:2013 en mano y para cada punto normativo, responda con total honestidad marcando con una x si cumple totalmente o parcialmente el requisito y de un porcentaje conforme a los valores de cumplimiento. Puede agregar un comentario para justificar su evaluación. En la demás hojas de cálculo se mostrará la brecha en forma visual y los análisis por numeral de la norma							
4. CONTEXTO DE LA ORGANIZACIÓN							
4.1 CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO							
La organización debe (5,3 NTC- ISO 31000:2011)	0%	25%	50%	75%	100%	N/A	OBSERVACIONES
Considerar las cuestiones externas pertinentes para su propósito y que afectan la capacidad para lograr los resultados previstos del SGSI							
4.2 COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS							
La organización debe determinar	0%	25%	50%	75%	100%	N/A	OBSERVACIONES
Partes interesadas que son pertinentes al SGSI							
Los requisitos de las partes interesadas pertinentes a la Seguridad de la información							
4.3 DETERMINACIÓN DEL ALCANCE DEL SGSI							
La organización debe	0%	25%	50%	75%	100%	N/A	OBSERVACIONES
Determinar los límites del SGSI							
Determinar la aplicabilidad del SGSI							
Considerar cuestiones Externas al determinar el alcance							

Gráfica 35. Hoja de diagnóstico, instrumento para determinar brechas de cumplimiento.

Fuente: Propia

Fueron incluidas las cláusulas 4 a 10 en un total de 242 filas, cada una de las cuales se califica de acuerdo a la escala de valoración propuesta en la tabla 11.

Tabla 11. Escala de valoración - diagnóstico inicial

Índice escala de valoración (i)	**% de cumplimiento (EV)**	**Descripción**
1	0%	No documentado/No existente
2	25%	Aplicado, no documentado
3	50%	Documentado, no aplicado
4	75%	Aplicado y documentado
5	100%	Aplicado, Documentado y Controlado
6	N/A	No aplica

La recolección de información y aplicación del instrumento se realizó a los cuatro sujetos de estudio de la Comuna Universidad.

El cálculo del cumplimiento por cláusula se determinó de la siguiente manera:

1. Total Debes normativos por cláusula:

$$T \quad = \sum_{i-1}^{5} D_i - D_6$$

Donde:

TDC = Total debes normativos por cláusula

DE = Cantidad total de Debes normativos

i = Índice de la escala de valoración

DE_6 = Cantidad total de exclusiones

Nota: Los valores DE_i y DE_6 se calculan por cláusula

2. Porcentaje de cumplimiento por cláusula:

$$P = \left(\sum_{i=1}^{5} (D_i \times E_i) \right) \div T$$

Donde:

PI = Porcentaje de implementación

DE = Cantidad total de Debes normativos

EV = Valor porcentual de cumplimiento

TDC = Total debes normativos por cláusula

i = Índice de la escala de valoración

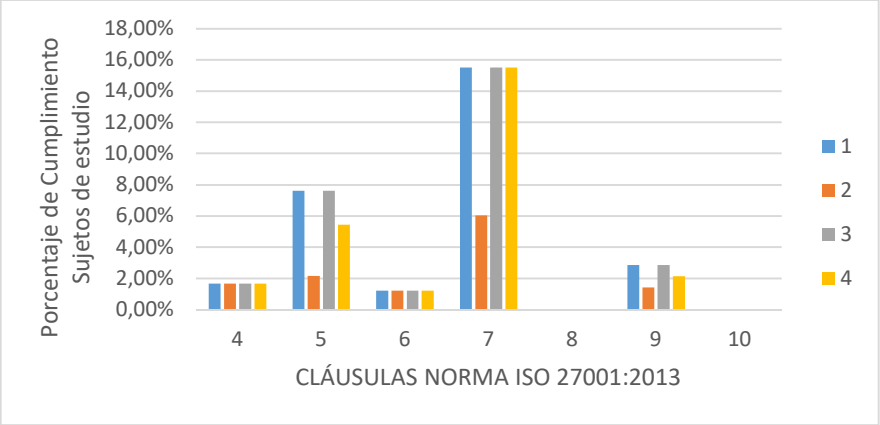
Nota: El valor DE_i se calcula por cláusula

La interpretación de los resultados obtenidos y la correlación de los datos se muestran en la tabla 12 y en el gráfico 36, estableciendo el punto de partida para el diseño del modelo del SGSI.

Tabla 12. Porcentaje de cumplimiento de los requisitos de la Norma NTC ISO/IEC 27001:2013.

Fuente: Propia

CLÁUSULAS	SUJETOS DE ESTUDIO COMUNA UNIVERSIDAD			
	1	2	3	4
4. Contexto de la organización	1,67%	1,67%	1,67%	1,67%
5 Liderazgo	7,61%	2,17%	7,61%	5,43%
6. Planificación	1,22%	1,22%	1,22%	1,22%
7. Soporte	15,52%	6,03%	15,52%	15,52%
8 Operación	0,00%	0,00%	0,00%	0,00%
9 Evaluación del desempeño	2,86%	1,43%	2,86%	2,14%
10. Mejora	0,00%	0,00%	0,00%	0,00%



Gráfica 36. Porcentaje de cumplimiento de los requisitos de la Norma ISO 27001:2013.

Fuente: Propia

A continuación, se presentará el análisis de los resultados para cada una de las cláusulas que hacen parte de la ISO/IEC 27001:2013.

Cláusula 4- Contexto de la organización: se evidencia que los sujetos de estudio cumplen con las disposiciones del MEN en relación con la seguridad de la información de las partes interesadas que intervienen en la prestación del servicio, mostrando una convergencia con los requisitos establecidos por la norma ISO 27001:2013, sin embargo, no fue posible evidenciar ningún tipo de actividad relacionada con el establecimiento, implementación, mantenimiento y mejora de un SGSI.

Cláusula 5 -Liderazgo: se evidencia que la alta dirección establece directrices relacionadas a la seguridad de la información, más por el cumplimiento de las disposiciones reglamentarias sobre tratamiento de datos personales de los niños y jóvenes que por la conciencia real de los riesgos presentes en la organización, de igual manera se evidencia que el sujeto de estudio 2 con menor cantidad de estudiantes, no evidencia el mismo nivel de compromiso que los sujetos de estudio que atienden mayor cantidad de población, siendo este hallazgo proporcional con los recursos presupuestales y tecnológicos disponibles.

Cláusula 6 -Planificación: En los 4 sujetos de estudio se evidencian que la alta dirección establece acciones conducentes a la mitigación de los riesgos, sin emplear para ello una metodología específica, sino que se realiza basado en la información suministrada por el personal contratado para atender los incidentes tanto de operatividad de la plataforma tecnológica como de seguridad que ya se han materializado. Las acciones preventivas tomadas se elaboran de manera empírica sin planificar la gestión de riesgos.

Cláusula 7 -Soporte: Ninguno de los 4 sujetos de estudio evidencia disponer de recursos presupuestales tendientes al establecimiento, implementación, mantenimiento y mejora de un SGSI, sin embargo, fue posible determinar que la competencia del recurso humano se valora directamente desde las Secretarias de Educación, no en los sujetos de estudio, limitando su función

al almacenamiento y actualización de las hojas de vida correspondientes. Con relación a la comunicación se evidenció que se tienen directrices específicas, conocidas por los colaboradores pero que no se encuentran documentadas, solo 3 de los sujetos de estudio mostraron acciones tendientes al control de información documentada.

Cláusula 8 -Operación: No se evidencia que los sujetos de estudio planifiquen los procesos necesarios para cumplir con los requisitos de seguridad de la información, al igual que el establecimiento de una metodología para la gestión de riegos y su valoración continua y documentada.

Cláusula 9 -Evaluación del desempeño: Todos los sujetos de estudio consideran la retroalimentación de las partes interesadas para evaluar el desempeño, sin embargo esta actividad se realiza solo por iniciativa de las partes interesadas más no por la organización en sí misma, quien establece los mecanismos de comunicación como herramienta para el cumplimiento de las disposiciones del MEN, sin embargo no fue posible evidenciar la documentación relacionada con dicha actividad, de igual manera no fue posible evidenciar la ejecución de auditorías internas que incentiven la mejora continua en seguridad de la información.

Cláusula 10 -Mejora: En la totalidad de los sujetos de estudio se evidencia incumplimiento total en el tratamiento de no conformidades y acciones correctivas, al igual que ausencia de acciones de mejora continua resultante de actividades relacionadas a la ejecución de auditorías internas.

Para determinar los porcentajes totales de implementación de la norma, se empleó la siguiente fórmula:

$$P = \sum_{i-1}^{5} (D_i \times E_i) \div \sum_{j-4}^{1} T_j$$

Donde:

PTI = Porcentaje de implementación total SGSI

DE = Cantidad total de Debes normativos

EV = Valor porcentual de cumplimiento

TDC = Total Debes normativos por cláusula

i = Índice de la escala de valoración

j = Índice de cláusula de la norma

Nota: El valor DE_i se calcula por la totalidad de cláusulas de la norma

Como resultado final del análisis de información y tal como se puede apreciar en la tabla 13, se concluye que ninguno de los sujetos de estudio adelanta acciones de manera activa para dar cumplimiento a lo dispuesto en el Decreto Único Reglamentario 1078/2015 con relación al Título 9 “Políticas y lineamientos de tecnologías de la información”, capítulo I “Estrategias de Gobierno en Línea”, Sección 2 “Componentes, instrumentos y responsables”, Art. 2.2.9.1.2.1 “Componentes” numeral 4 “Seguridad y privacidad de la información”, conforme lo revela el análisis de las brechas de cumplimiento.

Tabla 13. Brechas de cumplimiento de los sujetos de estudio.

SUJETOS DE ESTUDIO	PORCENTAJE OBTENIDO	BRECHAS DE CUMPLIMIENTO
1	4.79%	95.21%
2	2.10%	97.90%
3	4.79%	95.21%
4	4.34%	95.66%

El cálculo de la brecha de cumplimiento se realizó de acuerdo a la siguiente fórmula:

$$B \quad ha = P \quad - 100$$

4.1.2. Diagnóstico del grado de madurez del SGSI en las IED´s

Se emplearon como documentos guía el Modelo de seguridad y privacidad de la información y la Guía encuesta diagnóstico modelo de seguridad de la información para las entidades del estado expedidas por el MINTIC los cuales son complementarios para determinar el grado de madurez del SGSI en los sujetos de estudio.

El modelo propuesto por MINTIC consta de 5 componentes, los cuales se observan en la gráfica 37, que a su vez guardan relación con las cláusulas 4 a 10 de la Norma Internacional NTC ISO/IEC 27001:2013.

Gráfica 37. Cumplimiento para las entidades del orden territorial A, B y C.

Fuente Propia adaptado de guía el Modelo de seguridad y privacidad de la información (Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC, 2015, pág. 15)

Cada componente del modelo es correspondiente con los niveles de madurez definidos por el MINTIC, tal como se observa en la gráfica 38.

Gráfica 38. Niveles de madurez.

Fuente: (Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC, 2015, pág. 21)

La Guía encuesta diagnóstico modelo de seguridad de la información para las entidades del estado, establece los límites de calificación para cada nivel, como se observa en la gráfica 39.

Limites para las alertas para el Nivel Inicial / Gestionado			Limites para las alertas para el Nivel Definido			Limites para las alertas para el Nivel Gestionado Cuantitativamente			Limites para las alertas para el Nivel Optimizado		
Nivel de Cumplimiento	Limite Inferior	Limite Superior	Nivel de Cumplimiento	Limite Inferior	Limite Superior	Nivel de Cumplimiento	Limite Inferior	Limite Superior	Nivel de Cumplimiento	Limite Inferior	Limite Superior
Crítico	0	85	Crítico	0	87	Crítico	0	28	Crítico	0	31
Intermedio	86	125	Intermedio	88	147	Intermedio	29	47	Intermedio	32	53
Suficiente	126	210	Suficiente	147	245	Suficiente	48	80	Suficiente	54	90
FASE PLANEACIÓN			FASE DE IMPLEMENTACIÓN			FASE DE GESTIÓN			FASE DE MEJORA CONTINUA		

Gráfica 39. Límites para las alertas de los niveles de madurez.

Fuente: (Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC, 2015, pág. 8)

Una vez aplicado el instrumento y realizado el análisis de información se obtuvo los siguientes resultados relacionados en la gráfica 40:

Nivel de Cumplimiento	Inicial/Gestionado				Definido				Gestionado cuantitativamente				Optimizado			
	SUJETOS DE ESTUDIO															
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Crítico	11	0	11	49	40	20	40		0	0	0	17	10	0	10	
Intermedio							115									50
Suficiente																
	FASE PLANEACIÓN				FASE IMPLEMENTACIÓN				FASE GESTIÓN				FASE MEJORA CONTINUA			

Gráfica 40. Resultados aplicación diagnóstico, instrumento MINTIC.

Fuente: Propia

Es importante tener en cuenta que el documento de referencia de aplicación del diagnóstico, hace énfasis en la importancia de resaltar que “en tanto la entidad no obtenga el 100% de la calificación de cada Nivel no podrá avanzar a la siguiente, por tanto, se debe contestar cada pregunta basado en las actividades que la Entidad ha desarrollado para el MSPI”, (Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC, 2015, pág. 9).

De acuerdo a lo anterior los 4 sujetos de estudios se encuentran en Fase de Planeación en nivel Crítico lo cual refleja que no se han adelantado actividades tendientes a la definición de la estrategia metodológica que permita gestionar adecuadamente la seguridad de la información en cumplimiento con lo dispuesto en el Decreto Único Reglamentario 1078/2015 con relación al Título 9 “Políticas y lineamientos de tecnologías de la información”, capítulo I “Estrategias de Gobierno en Línea”, Sección 2 “Componentes, instrumentos y responsables”, Art. 2.2.9.1.2.1 “Componentes” numeral 4 “Seguridad y privacidad de la información”.

4.1.3. **Análisis de riesgos de las IED’s**

El proceso de identificación de riesgos en las IED’s ha tenido en cuenta las directrices de la Norma Internacional ISO/IEC 27005 en conjunción de elementos de la Norma NIST 800 –30, y se concretó a través de los pasos descritos a continuación.

4.1.3.1.Paso 1: Alcance

En concordancia con el numeral 4.3 de la norma NTC ISO 27001:2013 se determinó de manera conjunta con los rectores de las IED's quienes manifestaron su interés en el tratamiento de los riesgos del área de Secretaría Académica.

4.1.3.2.Paso 2: Inventario de activos

Se identificaron los activos del área de la Secretaría Académica que fueron comunes en las IED's de la Comuna Universidad, los resultados obtenidos se resumen en la tabla 14.

Tabla 14. Inventario de activos

NO ACTIVO	TIPO ACTIVO	DESCRIPCIÓN	OBSERVACIONES
1	Físico	Archivador	Almacenamiento de carpetas de los estudiantes, información de los docentes, certificados académicos, soportes escolares
2	Tecnológico	Computador	Registro de información académica en el software institucional y en el SIMAT, generación de certificados académicos y elaboración de informes
3	Tecnológico	Impresora	Impresión de los certificados de estudio, informes de rectoría, constancias
4	Tecnológico	Estabilizador	Protección del equipo para el procesamiento de información académica
5	Tecnológico	Teléfono	Atención al público, comunicación interna y externa
6	Humano	Secretaria Académica	Persona responsable del manejo y administración de la información de carácter académico de los estudiantes y soportes de desarrollo profesional de los docentes
7	Físico	Carpetas de soportes académicos de los estudiantes	Almacenamiento del historial académico de los estudiantes, desde la matrícula hasta el último año cursado
8	Físico	Carpetas con soportes de cualificación profesional y hoja de vida de los docentes	Almacenamiento de hojas de vida de los docentes y los soportes del desarrollo profesional
9	Físico	Oficina de Secretaría Académica	Lugar en el cual se llevan a cabo todas las actividades académicas y de almacenamiento de información física y digital

NO ACTIVO	TIPO ACTIVO	DESCRIPCIÓN	OBSERVACIONES
10	Lógico	Software de control académico	Programa de computadora que emplea la IED para administrar la información de los estudiantes, matriculas, asignación de grupos, docentes, registro de calificaciones, etc
11	Lógico	Sistema Operativo	Base operativa del equipo para el procesamiento de la información
12	Lógico	Paquete ofimático	Procesadores de texto, presentación en diapositivas, hojas de cálculo
13	Proceso	Matrícula	Registro de los estudiantes en el software de la IED y reporte en el SIMAT
14	Proceso	Actualización información docente	Actualización de los soportes de estudios de los docentes de la IED en su respectiva carpeta
15	Proceso	Emisión de certificados	Generación e impresión de certificados de notas y de estudio
16	Proceso	Registro de notas	Registro en el software de la IED de las notas de los estudiantes
17	Proceso	Generación de informes académicos	Creación y cruce de información para ser presentada en las reuniones de rectoría
18	Proceso	Generación de actas de grado	Creación de los listados de estudiantes para graduación y actas de grado
19	Físico	Unidad almacenamiento externo	Unidad para transportar información fuera de la oficina de la secretaría académica
20	Físico	Conexión de red PC Ethernet	Conexión de red para compartir archivos y acceso a internet
21	Humano	Rector	Persona responsable de adecuado funcionamiento del proceso de la IED

4.1.3.3.Paso 3: Factores de criticidad de los activos

Se identificaron los factores de criticidad de acuerdo a los criterios de disponibilidad, integridad y seguridad que se observan en gráfica 41, pero es posible que la IED determine la necesidad de incorporar algunos criterios adicionales.

CRITERIO	FACTOR	CUESTIONAMIENTO
DISPONIBILIDAD	FINANCIERO	¿Es posible que se genere afectación financiera por falta de disponibilidad del activo?
	LEGAL	¿Es posible que se genere afectación legal por la falta de disponibilidad del activo?
	IMAGEN	¿Es posible que se genere afectación a la imagen de la IED y la satisfacción del cliente por falta de disponibilidad del activo?
INTEGRIDAD	FINANCIERO	¿Es posible que se genere afectación financiera por cambios no autorizados en el activo?
	LEGAL	¿Es posible que se genere afectación legal por cambios no autorizados en el activo?
	IMAGEN	¿Es posible que se genere afectación a la imagen de la IED y la satisfacción del cliente por cambios no autorizados en el activo?
CONFIDENCIALIDAD	FINANCIERO	¿Es posible que se genere afectación financiera por divulgación no autorizada de información sensible?
	LEGAL	¿Es posible que se genere afectación legal por divulgación no autorizada de información sensible?
	IMAGEN	¿Es posible que se genere afectación a la imagen de la IED y la satisfacción del cliente por divulgación no autorizada de información sensible?

Gráfica 41. Factores para determinar la criticidad de los activos

Fuente: propia

4.1.3.4.Paso 4: Niveles de criticidad de los activos

CRITERIO DE EVALUACIÓN	CALIFICACIÓN	CRITICIDAD
El activo compromete en un alto grado la integridad y/o confidencialidad y/o disponibilidad de la información	>=33%	ALTO
El activo compromete en un nivel medio la integridad y/o confidencialidad y/o disponibilidad de la información	22%	MEDIO
El activo compromete en un nivel bajo la integridad y/o confidencialidad y/o disponibilidad de la información	11%	BAJO
El activo no compromete la integridad, confidencialidad y disponibilidad de la información	0%	NO CRITICO

Gráfica 42. Niveles de criticidad de los activos

Fuente: propia

La calificación de los factores de criticidad de los activos, se da en el rango 0 a 1 sin fracciones, por cuanto el máximo valor posible que pueden obtener cada uno de los factores es 9, la criticidad del activo (ver gráfica 42), se calcula a partir de la división de la sumatoria de los valores asignados a los factores valorados del activo en la calificación máxima posible.

$$N \quad = \sum C \quad \div M \quad (C \quad)$$

Donde:

NCA = Nivel de criticidad del activo

CFA = Calificación de factores para el activo

Max(CFA) = Máximo valor posible de calificación de los factores para el activo

Los resultados obtenidos de la criticidad de los activos del área de Secretaría Académica de las IED's se relacionan en la siguiente tabla.

Tabla 15. Criticidad de activos en las IED's

No. Activo	Valoración nivel de criticidad de los activos									Criticidad
	Confidencialidad			Integridad			Disponibilidad			
	Financ	Legal	Imagen	Financ	Legal	Imagen	Financ	Legal	Imagen	
1	0	1	1	0	1	1	0	1	1	67%
2	1	1	1	1	1	1	1	1	1	100%
3	0	0	0	0	0	0	0	0	1	11%
4	0	0	0	0	0	0	0	0	1	11%
5	0	1	0	0	0	0	0	0	1	22%
6	1	1	1	1	1	1	1	1	1	100%
7	0	1	1	0	1	1	1	1	1	78%
8	0	0	1	0	0	1	0	1	0	33%
9	0	0	0	0	0	1	0	0	1	22%
10	1	1	1	0	1	0	0	0	1	56%
11	0	0	0	0	0	0	1	0	1	22%
12	0	0	0	0	0	0	0	1	1	22%
13	1	1	1	0	1	0	1	1	1	78%
14	0	1	0	0	1	0	0	0	0	22%
15	0	0	0	0	0	1	0	1	0	22%
16	0	0	1	0	0	1	0	1	1	44%
17	0	0	1	0	0	0	0	1	0	22%
18	0	1	1	0	1	1	1	1	1	78%
19	0	0	0	0	0	0	0	0	1	11%
20	0	1	1	0	1	0	0	1	1	56%
21	1	1	1	1	1	1	1	1	1	100%

4.1.3.5.Paso 5: Escenarios de riesgo

La tabla 16 resume los escenarios de riesgos identificados en relación a los activos, así como el posible origen del mismo identificándolos como DE = deliberado, AC = accidental y AMB = ambiental.

Tabla 16. Escenarios de riesgo de las IED’s.

No	RIESGO	ORIGEN
1	Afectación legal por pérdida de información del computador de la Secretaría Académica de la IED que almacena la información de los estudiantes y contiene los registros y formatos de las actas de grado y certificados de estudio	DE, AC, AMB
2	Afectación legal por pérdida de la información de los estudiantes y/o docentes por deficiencias en los procesos de inducción y capacitación de la Secretaria Académica de la institución	DE, AC
3	Afectación legal por pérdida mediante sustracción de las carpetas que contienen los soportes académicos de los estudiantes	DE
4	Afectación legal por pérdida mediante sustracción de las carpetas que contienen los soportes de cualificación profesional de los docentes	DE
5	Afectación legal por pérdida de la información del software de control académico de la Institución	DE, AC, AMB
6	Afectación legal por errores en el proceso de matrícula al registrar la información de los estudiantes en el software de la IED y /o en el SIMAT, por parte de personal no idóneo o con falta de entrenamiento	DE, AC
7	Acceso a información confidencial de los estudiantes mediante fotografías o copias no autorizadas de las carpetas almacenadas en el archivo, empleando dispositivos móviles por falta de control en el acceso al mismo	DE
8	Acceso a información confidencial mediante la sustracción de información del computador de la secretaría académica empleando conexión no autorizada a través de dispositivos móviles o unidades de almacenamiento extraíble	DE
9	Acceso a información confidencial de los estudiantes a través de dispositivos móviles durante el proceso de registro de calificaciones en el software de la IED, por exposición del escritorio de trabajo de la secretaria académica a personal no autorizado	DE, AC

No	RIESGO	ORIGEN
10	Acceso a información confidencial mediante la interceptación de la red interna de la secretaría académica a través del cableado del cielo raso que queda expuesto fuera de las oficinas por falta de mecanismos de protección	DE
11	Tratamiento erróneo de la información de los estudiantes en el software de control de la IED y/o en el SIMAT afectando los reportes requeridos por la Secretaría de Educación y los informes a la rectoría por falta de entrenamiento del personal	DE, AC
12	Alteración de la información académica de los estudiantes por errores en el tratamiento de la información por parte del software de control académico de la IED	AC
13	Alteración del proceso de generación de actas de grado, mediante la expedición errónea y/o no autorizada de actas con sello de la institución con participación del personal de la secretaría académica	DE
14	Divulgación no autorizada por parte del personal de la secretaría académica de la información de personal de los estudiantes y/o docentes a terceros	DE, AC
15	Tratamiento erróneo de la información de los estudiantes y/o docentes tanto digital como física por deficiencias en los canales de comunicación de las políticas administrativas establecidas por el rector de la institución	DE, AC
16	Acceso no autorizado al área de archivo de las carpetas con la información de los estudiantes y/o docentes de la IED, por falta de mecanismos de control de acceso de personal externo	DE, AC
17	Acceso no autorizado al computador del área de secretaría académica por falta de mecanismos de control de acceso a personal externo y/o falta de control en la atención al público	DE, AC
18	Acceso no autorizado al software de control académico por ausencia de mecanismos de control en el puesto de trabajo de la secretaria académica	DE, AC
19	Acceso no autorizado al proceso de matrícula de los estudiantes en el software de la IED y/o al SIMAT por ausencia de políticas sobre el manejo confidencial de la información de registro académico	DE, AC
20	Acceso no autorizado al proceso de registro de calificaciones de los estudiantes en el software de la IED por ausencia de políticas sobre el manejo confidencial de la información de registro académico	DE, AC

No	RIESGO	ORIGEN
21	Acceso no autorizado a las plantillas institucionales para la generación de actas de grado por falta de controles para el uso del computador de la secretaría académica	DE, AC
22	Acceso no autorizado a información física y/o digital de los estudiantes y docentes por falta de políticas de acceso para personal no autorizado a la Institución y al área de secretaría académica por parte del rector	DE, AC
23	Acceso a información confidencial física y/o digital de estudiantes y docentes por parte de los ex colaboradores de la institución por falta de controles para la eliminación de usuarios y políticas de acceso a la planta física de personal retirado de la institución	DE, AC
24	Errores en el tratamiento de información por ausencia de entrenamiento y/o instrumentos de consulta que permitan que el nuevo personal del área de secretaría académica consulte las particularidades de los procesos adelantados con la información de estudiantes y docentes, tanto en el manejo del archivo físico como en el software de la IED por falta de exigencia de la rectoría en la entrega adecuada del puesto de trabajo por parte de los funcionarios retirados, así como la solicitud de manuales que permitan saber las actividades propias del proceso	DE, AC
25	Hurto de dispositivos de almacenamiento, procesamiento y/o impresoras del área de secretaría académica por falta de controles de acceso a la IED y al área en horarios de atención al público	DE
26	Fallos en el equipo de cómputo de la secretaría académica por uso inadecuado del recurso por parte del personal del área	DE, AC
27	Averías en el equipo de cómputo de la secretaría académica por falta de mantenimiento preventivo programado por la rectoría	DE, AC
28	Averías en el equipo de cómputo de la secretaría académica por el no reporte oportuno de las incidencias por parte de la secretaria académica	DE, AC
29	Demora en la atención de los usuarios por problemas de tiempo en el procesamiento de información del equipo de cómputo de la secretaría académica	DE, AC
30	Demora en la atención de los usuarios por problemas relacionados con la idoneidad en el manejo del equipo de cómputo y/o software para el control académico de la IED por parte de la secretaria académica	DE, AC

No	RIESGO	ORIGEN
31	Demora en el proceso de atención de los usuarios por desconocimiento e idoneidad para adelantar el proceso de matrícula de los estudiantes	DE, AC
32	Demora en el proceso de atención de los usuarios por retraso en el proceso de ingreso de las calificaciones reportadas por los docentes al sistema de control de la IED por parte de la secretaria académica	DE
33	Desatención del equipo de procesamiento de datos y archivo por citaciones a reuniones constantes en horarios habilitados para atención al público por parte del rector	DE
34	Entrega de plantillas institucionales a personal no autorizado por parte de la secretaria académica	DE
35	Fallos o demoras en la atención del público por afectación de software malicioso en el equipo de cómputo de la secretaría académica	DE, AC
36	Afectación del equipo de la secretaría académica por software malicioso a causa del uso inadecuado del recurso por parte del personal de la secretaría académica	DE, AC
37	Afectaciones de las comunicaciones por infección de software malicioso que incide en los drivers de la tarjeta de red del computador de la secretaría académica	DE, AC
38	Pérdida del archivo físico de los estudiantes y docentes por ocurrencia de desastre natural (terremoto, derrumbe, inundación, etc.)	AMB
39	Pérdida del equipo de cómputo e información digital de la secretaría académica por ocurrencia de desastre natural (terremoto, derrumbe, inundación, etc.)	AMB
40	Pérdida de las comunicaciones para el reporte a la Secretaría de Educación y/o entidades externas por daños en los sistemas de comunicación ocasionados por desastres naturales	AMB
41	Pérdida de información en el equipo de cómputo de la secretaría académica por fallos del fluido eléctrico	AC, AMB
42	Daño en el software de control académico por fallos en el fluido eléctrico	AC, AMB
43	Parálisis del proceso de matrícula por fallos en el fluido eléctrico	AC, AMB
44	Retrasos en el proceso de ingreso de calificaciones por fallos en el fluido eléctrico	AC, AMB
45	Daño en el archivo y/o equipos de cómputo e información digital por fuego provocado	DE

No	RIESGO	ORIGEN
46	Afectación física en el personal del área de secretaría académica por fuego provocado y ausencia de planes de emergencia y/o rutas adecuadas de evacuación	DE
47	Deterioro del archivo físico de los estudiantes y los docentes por corrosión provocada por humedad	AMB
48	Incumplimiento en los reportes al SIMAT, a la plataforma del ICFES para las pruebas SABER y Secretaría de Educación por fallos en los dispositivos que permiten la prestación del servicio de Internet	DE, AC, AMB
49	Interceptación de datos de los estudiantes por infección con software espía por deficiencias en los mecanismos de protección tales como antivirus y antimalware	DE, AC
50	Divulgación de la información de los estudiantes y/o docentes por medio de la práctica inadecuada de desecho de información reciclada por parte de la secretaria académica	DE, AC
51	Divulgación de la información de los estudiantes y/o docentes por falta de políticas y mecanismos para la adecuada disposición de los desechos	DE, AC
52	Fallos en el funcionamiento del equipo de cómputo de la secretaría académica por instalación de software pirata, ocasionado por falta de políticas con los proveedores, y el personal de la IED	DE, AC
53	Divulgación y daño en la información confidencial de los estudiantes y/o docentes por retaliaciones políticas en periodos de elecciones por falta de políticas de confidencialidad	DE
54	Exposición de las contraseñas de acceso a los equipos de cómputo y sistemas de información por falta de medidas de prevención, uso adecuado y preservación de las mismas	DE
55	Demora en el restablecimiento del servicio por fallos relacionados a la extracción de copias de seguridad y pruebas de las mismas	DE

4.1.3.6.Paso 6: Calificación de la probabilidad

Como resultado de las entrevistas realizadas a los directivos de las IED's y a las características particulares de las instituciones educativas analizadas, se propone la calificación de probabilidad relacionada en la gráfica 44.

VALOR	PROBABILIDAD	DESCRIPCIÓN
1	BAJO	Menos de 2 veces al año o baja probabilidad de ocurrencia
2	MEDIO	Entre 2 y 5 veces al año o mediana probabilidad de ocurrencia
3	ALTO	Más de 5 veces al año o alta probabilidad de ocurrencia

Gráfica 43. Calificación de probabilidad

Fuente: propia

4.1.3.7.Paso 7: Impacto potencial

El impacto potencial fue adaptado de los propuestos por la norma NIST 800 – 30 y se resume en la gráfica 45.

CRITERIO	BAJO	MODERADO	ALTO
	1	2	3
CONFIDENCIALIDAD	La divulgación no autorizada de información de estudiantes y/o docentes podría tener un efecto adverso limitado en las operaciones de la IED, los activos o sus individuos	Se podría esperar que la divulgación no autorizada de información de estudiantes y/o docentes tenga un efecto adverso serio sobre las operaciones de la IED, los activos o sus individuos.	La divulgación no autorizada de información de estudiantes y/o docentes podría tener un efecto adverso grave o catastrófico en las operaciones de la IED, los activos o individuos.
INTEGRIDAD	La modificación o destrucción imprevista de información académica, personas, herramientas, dispositivos, etc podrían tener un efecto adverso limitado en las operaciones de la IED, los activos o sus individuos	La modificación o destrucción imprevista de información académica, personas, herramientas, dispositivos, etc podrían tener un efecto adverso serio en las operaciones de la IED, los activos o sus individuos	La modificación o destrucción imprevista de información académica, personas, herramientas, dispositivos, etc podrían tener un efecto adverso grave o catastrófico en las operaciones de la IED, los activos o sus individuos
DISPONIBILIDAD	La interrupción del acceso o uso de información académica o a un sistema de información podría tener un efecto adverso limitado en las operaciones de la IED, los activos o sus individuos.	La interrupción del acceso o uso de información académica o a un sistema de información podría tener un efecto adverso serio en las operaciones de la IED, los activos o sus individuos.	La interrupción del acceso o uso de información académica o a un sistema de información podría tener un efecto adverso grave o catastrófico en las operaciones de la IED, los activos o sus individuos.

Gráfica 44. Impacto potencial, adaptado de NIST 800 – 30

4.1.3.8.Paso 8: Vulnerabilidad inherente

Para hallar la vulnerabilidad inherente se consignan los valores pertinentes a la probabilidad y el impacto para cada uno de los factores relacionados con confidencialidad, integridad y disponibilidad, sumando la totalidad los valores asignados.

$$I_{Total} = I_c + I_i + I_d$$

Donde:

ITotal = Impacto total

Ic = Calificación impacto en la confidencialidad

Ii = Calificación de impacto en la integridad

Id = Calificación de impacto en la disponibilidad

Para calcular la vulnerabilidad inherente:

Determine la vulnerabilidad en cada uno de los factores como:

$$V_{Ic} = (P \times I_c)/M_{(P \times I_c)}$$

Donde:

VIc = Vulnerabilidad Inherente Confidencialidad

Ic = Calificación impacto en la confidencialidad

P = Probabilidad

Max(P X Ic) = Máximo valor posible de la probabilidad por el impacto, en esta metodología el máximo valor de la probabilidad es 3, y el máximo valor del impacto es 3, por tanto el denominador de la anterior ecuación es 9.

De igual manera se procede con los otros dos factores.

El cálculo de la vulnerabilidad inherente total se halla de:

$$V \quad = (P \times (I_{\iota} + I_{\imath} + I_{\iota}) \div M \quad (P \times (I_{\iota} + I_{\imath} + I_{\iota}))$$

Donde:

VIt = Vulnerabilidad inherente total

$M \quad (P \times (I_{\iota} + I_{\imath} + I_{\iota}))$ = Máximo valor posible de la probabilidad por el impacto, en esta metodología el máximo valor de la probabilidad es 3, y el máximo valor de la combinación de los impactos es 9, por tanto, el denominador de la anterior ecuación es 27.

La vulnerabilidad inherente se muestra en la siguiente tabla.

Tabla 17. Vulnerabilidad inherente – Secretaría Académica IED's

Fuente: propia

NO	ESCENARIO DE RIESGO	PROBA-BILIDAD	IMPACTO				VULNERABILIDAD INHERENTE			
			C	I	D	TOTAL	C	I	D	TOTAL
1	Afectación legal por pérdida de información del computador de la Secretaría Académica de la IED que almacena la información de los estudiantes y contiene los registros y formatos de las actas de grado y certificados de estudio	1	3	3	3	9	33%	33%	33%	33%
2	Afectación legal por pérdida de la información de los estudiantes y/o docentes por deficiencias en los procesos de inducción y capacitación de la Secretaria Académica de la institución	2	3	2	2	7	67%	44%	44%	52%
3	Afectación legal por pérdida mediante sustracción de las carpetas que contienen los soportes académicos de los estudiantes	3	3	3	3	9	100%	100%	100%	100%
4	Afectación legal por pérdida mediante sustracción de las carpetas que contienen los soportes de cualificación profesional de los docentes	3	3	3	3	9	100%	100%	100%	100%
5	Afectación legal por pérdida de la información del software de control académico de la Institución	2	1	3	3	7	22%	67%	67%	52%
6	Afectación legal por errores en el proceso de matrícula al registrar la información de los estudiantes en el software de la IED y /o en el SIMAT, por parte de personal no idóneo o con falta de entrenamiento	3	1	3	1	5	33%	100%	33%	56%

NO	ESCENARIO DE RIESGO	PROBA-BILIDAD	IMPACTO				VULNERABILIDAD INHERENTE			
			C	I	D	TOTAL	C	I	D	TOTAL
7	Acceso a información confidencial de los estudiantes y/o docentes mediante fotografías o copias no autorizadas de las carpetas almacenadas en el archivo, empleando dispositivos móviles por falta de control en el acceso al mismo	3	3	1	1	5	100%	33%	33%	56%
8	Acceso a información confidencial mediante la sustracción de información del computador de la secretaría académica empleando conexión no autorizada a través de dispositivos móviles o unidades de almacenamiento extraíble	3	3	3	1	7	100%	100%	33%	78%
9	Acceso a información confidencial de los estudiantes a través de dispositivos móviles durante el proceso de registro de calificaciones en el software de la IED, por exposición del escritorio de trabajo de la secretaria académica a personal no autorizado	2	1	1	2	4	22%	22%	44%	30%
10	Acceso a información confidencial mediante la interceptación de la red interna de la secretaría académica a través del cableado del cielo raso que queda expuesto fuera de las oficinas por falta de mecanismos de protección	3	3	3	2	8	100%	100%	67%	89%
11	Tratamiento erróneo de la información de los estudiantes en el software de control de la IED y/o en el SIMAT afectando los reportes requeridos por la Secretaría de Educación y los informes a la rectoría por falta de entrenamiento del personal	3	1	3	1	5	33%	100%	33%	56%
12	Alteración de la información académica de los estudiantes por errores en el tratamiento de la información por parte del software de control académico de la IED	1	2	3	3	8	22%	33%	33%	30%
13	Alteración del proceso de generación de actas de grado, mediante la expedición errónea y/o no autorizada de actas con sello de la institución con participación del personal de la secretaría académica	2	2	3	1	6	44%	67%	22%	44%
14	Divulgación no autorizada por parte del personal de la secretaría académica de la información de personal de los estudiantes y/o docentes a terceros	2	3	1	1	5	67%	22%	22%	37%
15	Tratamiento erróneo de la información de los estudiantes y/o docentes tanto digital como física por deficiencias en los canales de comunicación de las políticas administrativas establecidas por el rector de la institución	3	1	2	1	4	33%	67%	33%	44%
16	Acceso no autorizado al área de archivo de las carpetas con la información de los estudiantes y/o docentes de la IED, por falta de mecanismos de control de acceso de personal externo	2	3	3	3	9	67%	67%	67%	67%
17	Acceso no autorizado al computador del área de secretaría académica por falta de mecanismos de control de acceso a personal externo y/o falta de control en la atención al público	3	3	3	3	9	100%	100%	100%	100%

NO	ESCENARIO DE RIESGO	PROBA-BILIDAD	IMPACTO				VULNERABILIDAD INHERENTE			
			C	I	D	TOTAL	C	I	D	TOTAL
18	Acceso no autorizado al software de control académico por ausencia de mecanismos de control en el puesto de trabajo de la secretaria académica	3	3	3	3	9	100%	100%	100%	100%
19	Acceso no autorizado al proceso de matrícula de los estudiantes en el software de la IED y/o al SIMAT por ausencia de políticas sobre el manejo confidencial de la información de registro académico	2	3	3	3	9	67%	67%	67%	67%
20	Acceso no autorizado al proceso de registro de calificaciones de los estudiantes en el software de la IED por ausencia de políticas sobre el manejo confidencial de la información de registro académico	3	3	3	3	9	100%	100%	100%	100%
21	Acceso no autorizado a las plantillas institucionales para la generación de actas de grado por falta de controles para el uso del computador de la secretaría académica	2	1	1	1	3	22%	22%	22%	22%
22	Acceso no autorizado a información física y/o digital de los estudiantes y docentes por falta de políticas de acceso para personal no autorizado a la Institución y al área de secretaría académica por parte del rector	2	3	3	3	9	67%	67%	67%	67%
23	Acceso a información confidencial física y/o digital de estudiantes y docentes por parte de los ex colaboradores de la institución por falta de controles para la eliminación de usuarios y políticas de acceso a la planta física de personal retirado de la institución	3	3	3	3	9	100%	100%	100%	100%
24	Errores en el tratamiento de información por ausencia de entrenamiento y/o instrumentos de consulta que permitan que el nuevo personal del área de secretaría académica consulte las particularidades de los procesos adelantados con la información de estudiantes y docentes, tanto en el manejo del archivo físico como en el software de la IED por falta de exigencia de la rectoría en la entrega adecuada del puesto de trabajo por parte de los funcionarios retirados, así como la solicitud de manuales que permitan saber las actividades propias del proceso	3	2	3	2	7	67%	100%	67%	78%
25	Hurto de dispositivos de almacenamiento, procesamiento y/o impresoras del área de secretaría académica por falta de controles de acceso a la IED y al área en horarios de atención al público	3	3	1	2	6	100%	33%	67%	67%
26	Fallos en el equipo de cómputo de la secretaría académica por uso inadecuado del recurso por parte del personal del área	2	1	3	3	7	22%	67%	67%	52%
27	Averías en el equipo de cómputo de la secretaría académica por falta de mantenimiento preventivo programado por la rectoría	2	1	3	3	7	22%	67%	67%	52%

NO	ESCENARIO DE RIESGO	PROBA-BILIDAD	IMPACTO				VULNERABILIDAD INHERENTE			
			C	I	D	TOTAL	C	I	D	TOTAL
28	Averías en el equipo de cómputo de la secretaría académica por el no reporte oportuno de las incidencias por parte de la secretaria académica	3	1	3	3	7	33%	100%	100%	78%
29	Demora en la atención de los usuarios por problemas de tiempo en el procesamiento de información del equipo de cómputo de la secretaría académica	3	1	1	3	5	33%	33%	100%	56%
30	Demora en la atención de los usuarios por problemas relacionados con la idoneidad en el manejo del equipo de cómputo y/o software para el control académico de la IED por parte de la secretaria académica	3	1	1	3	5	33%	33%	100%	56%
31	Demora en el proceso de atención de los usuarios por desconocimiento e idoneidad para adelantar el proceso de matrícula de los estudiantes	3	1	1	3	5	33%	33%	100%	56%
32	Demora en el proceso de atención de los usuarios por retraso en el proceso de ingreso de las calificaciones reportadas por los docentes al sistema de control de la IED por parte de la secretaria académica	3	1	1	3	5	33%	33%	100%	56%
33	Demora en el proceso de atención a los usuarios por citaciones a reuniones constantes en horarios habilitados para atención al público por parte del rector	3	1	1	3	5	33%	33%	100%	56%
34	Entrega de plantillas institucionales a personal no autorizado por parte de la secretaria académica	2	1	1	1	3	22%	22%	22%	22%
35	Fallos o demoras en la atención del público por afectación de software malicioso en el equipo de cómputo de la secretaría académica	3	3	3	3	9	100%	100%	100%	100%
36	Afectación del equipo de la secretaría académica por software malicioso a causa del uso inadecuado del recurso por parte del personal de la secretaría académica	2	3	3	3	9	67%	67%	67%	67%
37	Afectaciones de las comunicaciones por infección de software malicioso que incide en los drivers de la tarjeta de red del computador de la secretaría académica	2	3	3	3	9	67%	67%	67%	67%
38	Pérdida del archivo físico de los estudiantes y docentes por ocurrencia de desastre natural (terremoto, derrumbe, inundación, etc.)	2	1	3	3	7	22%	67%	67%	52%
39	Pérdida del equipo de cómputo e información digital de la secretaría académica por ocurrencia de desastre natural (terremoto, derrumbe, inundación, etc.)	2	1	3	3	7	22%	67%	67%	52%
40	Pérdida de las comunicaciones para el reporte a la Secretaría de Educación y/o entidades externas por daños en los sistemas de comunicación ocasionados por desastres naturales	3	1	1	3	5	33%	33%	100%	56%
41	Pérdida de información en el equipo de cómputo de la secretaría académica por fallos del fluido eléctrico	3	1	3	3	7	33%	100%	100%	78%

NO	ESCENARIO DE RIESGO	PROBA-BILIDAD	IMPACTO				VULNERABILIDAD INHERENTE			
			C	I	D	TOTAL	C	I	D	TOTAL
42	Daño en el software de control académico por fallos en el fluido eléctrico	3	1	3	3	7	33%	100%	100%	78%
43	Parálisis del proceso de matrícula por fallos en el fluido eléctrico	3	1	1	3	5	33%	33%	100%	56%
44	Retrasos en el proceso de ingreso de calificaciones por fallos en el fluido eléctrico	3	1	1	3	5	33%	33%	100%	56%
45	Daño en el archivo y/o equipos de cómputo e información digital por fuego provocado	1	1	3	3	7	11%	33%	33%	26%
46	Afectación física en el personal del área de secretaría académica por fuego provocado y ausencia de planes de emergencia y/o rutas adecuadas de evacuación	2	1	1	3	5	22%	22%	67%	37%
47	Deterioro del archivo físico de los estudiantes y los docentes por corrosión provocada por humedad	3	1	3	3	7	33%	100%	100%	78%
48	Incumplimiento en los reportes al SIMAT, a la plataforma del ICFES para las pruebas SABER y Secretaría de Educación por fallos en los dispositivos que permiten la prestación del servicio de Internet	2	1	1	3	5	22%	22%	67%	37%
49	Interceptación de datos de los estudiantes por infección con software espía por deficiencias en los mecanismos de protección tales como antivirus y antimalware	3	3	3	3	9	100%	100%	100%	100%
50	Divulgación de la información de los estudiantes y/o docentes por medio de la práctica inadecuada de desecho de información reciclada por parte de la secretaria académica	3	3	1	1	5	100%	33%	33%	56%
51	Divulgación de la información de los estudiantes y/o docentes por falta de políticas y mecanismos para la adecuada disposición de los desechos	3	3	1	1	5	100%	33%	33%	56%
52	Fallos en el funcionamiento del equipo de cómputo de la secretaría académica por instalación de software pirata, ocasionado por falta de políticas con los proveedores, y el personal de la IED	3	3	3	3	9	100%	100%	100%	100%
53	Divulgación y daño en la información confidencial de los estudiantes y/o docentes por retaliaciones políticas en periodos de elecciones por falta de políticas de confidencialidad	3	3	3	3	9	100%	100%	100%	100%
54	Exposición de las contraseñas de acceso a los equipos de cómputo y sistemas de información por falta de medidas de prevención, uso adecuado y preservación de las mismas	3	3	3	3	9	100%	100%	100%	100%
55	Demora en el restablecimiento del servicio por fallos relacionados a la extracción de copias de seguridad y pruebas de las mismas	3	1	3	3	7	33%	100%	100%	78%

4.1.3.9.Paso 9: Aceptabilidad del riesgo

Como resultado de las entrevistas realizadas a los directivos de las IED's y a las características particulares de las instituciones educativas analizadas, se propone la siguiente tabla de aceptabilidad del riesgo. Cada criterio de aceptación se identifica con color verde, amarillo y rojo respectivamente.

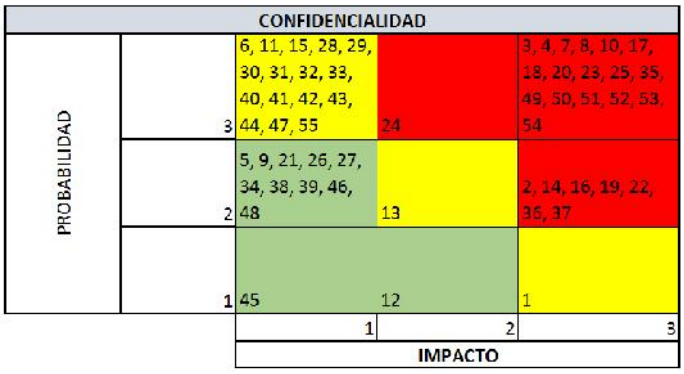
Tabla 18. Aceptabilidad del riesgo

Fuente: propia

Identificación	Criterio	Calificación
Verde	Aceptable	<= 25%
Amarillo	Tolerable	>25% y <= 50%
Rojo	Inaceptable	>50%

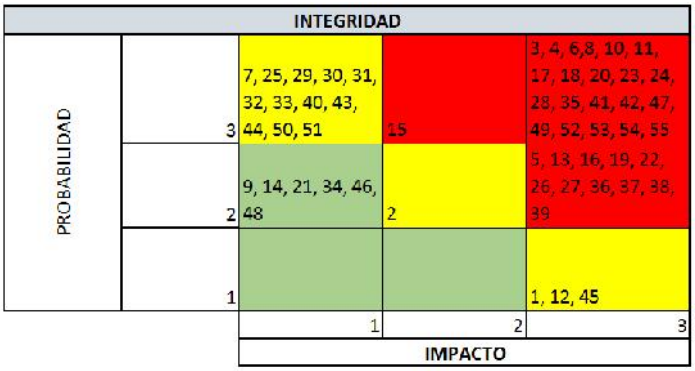
4.1.3.10. Paso 10: Mapas de temperatura de vulnerabilidad inherente

Las gráficas 45, 46, 47, 48 y 49 ubican los valores resultantes de la calificación de la vulnerabilidad inherente, para confidencialidad, integridad, disponibilidad y total respectivamente, teniendo en cuenta el eje X = Impacto y el eje Y = Probabilidad.



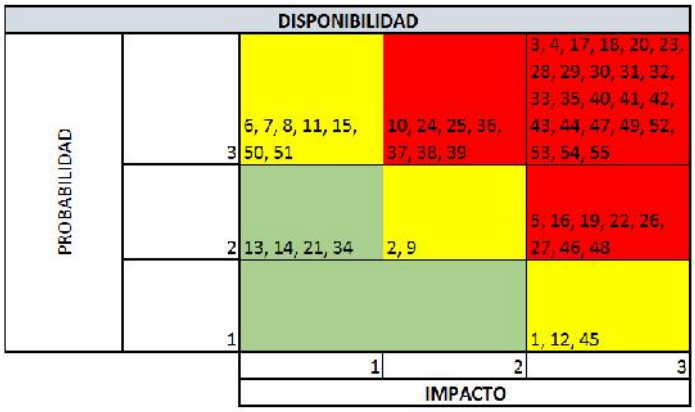
Gráfica 45. Vulnerabilidad inherente confidencialidad

Fuente: propia



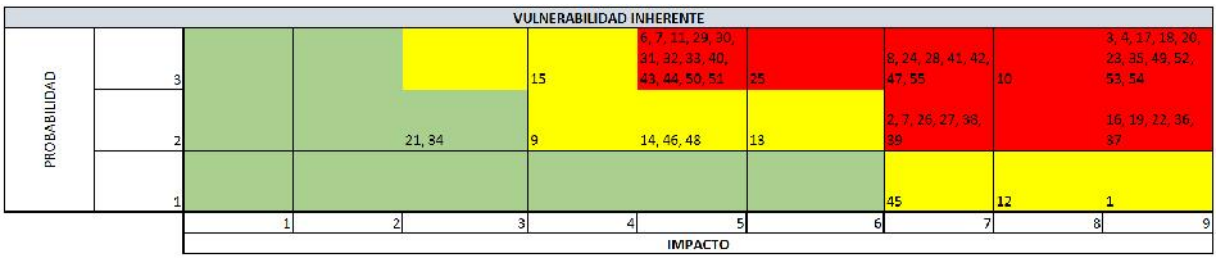
Gráfica 46. Vulnerabilidad inherente integridad

Fuente: propia



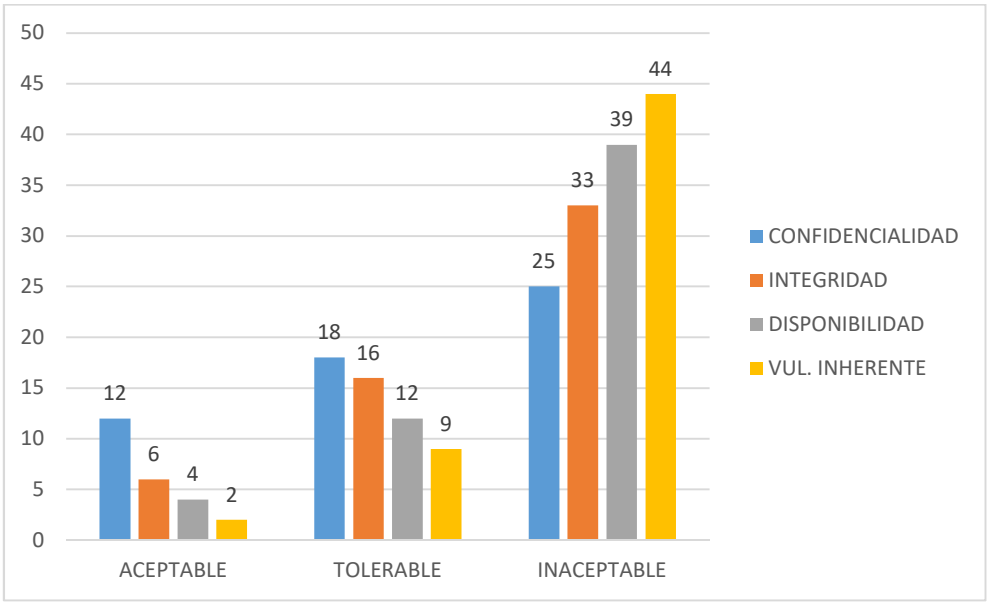
Gráfica 47. Vulnerabilidad inherente disponibilidad

Fuente: propia



Gráfica 48. Vulnerabilidad inherente total

Fuente: propia



Gráfica 49. Cantidad de riesgos por criterio y por aceptabilidad en el análisis de la vulnerabilidad inherente

Fuente: propia

4.1.3.11. Paso 11: Controles actuales identificados en las IED's

En la siguiente tabla se listan los controles identificados en la IED y que se emplean actualmente.

Tabla 19. Controles actuales

NO RIESGO	ESCENARIO DE RIESGO	COD CTRL	CONTROL ACTUAL
1	Afectación legal por pérdida de información del computador de la Secretaría Académica de la IED que almacena la información de los estudiantes y contiene los registros y formatos de las actas de grado y certificados de estudio	A.5.1.1 A.11.1.2	1. Control de acceso de personas externas a la IED mediante personal de seguridad
		A.11.1.1	2. Control de acceso a la IED mediante mallas, muros y cercados
		A.5.1.1 A.9.4.3	3. Protección con contraseñas del equipo de secretaría académica
2	Afectación legal por pérdida de la información de los estudiantes y/o docentes por deficiencias en los procesos de inducción y capacitación de la Secretaria Académica de la institución	A.7.1.2 A.12.1.1	1. Manual de funciones y responsabilidades
		A.12.1.1 A.12.1.2 A.7.2.2	2. Capacitaciones con las entidades correspondientes cuando se llevan a cabo cambios en la plataforma de ingreso de información del Ministerios de Educación Nacional, ICFES (Pruebas Saber PRO) y cuando se presentan cambios del Software Institucional previa aprobación de la Secretaría de Educación
3	Afectación legal por pérdida mediante sustracción de las carpetas que contienen los soportes académicos de los estudiantes	A.11.1.2	1. Control de acceso de personas externas a la IED mediante personal de seguridad
		A.11.1.1	2, Control de acceso a la IED mediante mallas, muros y cercados

NO RIESGO	ESCENARIO DE RIESGO	COD CTRL	CONTROL ACTUAL
		A.11.1.3	3. Ventanas con rejas de hierro para prevenir el acceso no autorizado de terceros
		A.5.1.1 A.9.1.1	4. Políticas rectorales sobre el acceso de estudiantes al área de archivo
		A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.6	5. Cámaras de Vigilancia
		A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.6	6. Sensores de movimiento
4	Afectación legal por pérdida mediante sustracción de las carpetas que contienen los soportes de cualificación profesional de los docentes	A.11.1.2	1. Control de acceso de personas externas a la IED mediante personal de seguridad
		A.11.1.1	2, Control de acceso a la IED mediante mallas, muros y cercados
		A.11.1.3	3. Ventanas con rejas de hierro para prevenir el acceso no autorizado de terceros
		A.5.1.1 A.9.1.1	4. Políticas rectorales sobre el acceso a la información de las hojas de vida de los docentes por parte de personal no autorizado
		A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.6	5. Cámaras de vigilancia

NO RIESGO	ESCENARIO DE RIESGO	COD CTRL	CONTROL ACTUAL
		A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.6	6. Sensores de movimiento
5	Afectación legal por pérdida de la información del software de control académico de la Institución	A.9.4.3	1. Protección con contraseñas del equipo de secretaría académica
		A.5.1.1 A.9.1.1	2. Políticas rectorales sobre el uso del equipo de cómputo de la secretaría académica por parte de personal no autorizado
6	Afectación legal por errores en el proceso de matrícula al registrar la información de los estudiantes en el software de la IED y /o en el SIMAT, por parte de personal no idóneo o con falta de entrenamiento	A.12.1.1 A.12.1.2 A.7.2.2	1. Capacitaciones con las entidades correspondientes cuando se llevan a cabo cambios en la plataforma de ingreso de información del Ministerios de Educación Nacional, ICFES (Pruebas Saber PRO) y cuando se presentan cambios del Software Institucional previa aprobación de la Secretaría de Educación.
		A.16.1.2 A.16.1.3	2. Entrega periódica de informes de manera verbal y/o escrita a la rectoría sobre las novedades presentadas en las plataformas de gestión de información empleadas
7	Acceso a información confidencial de los estudiantes y/o docentes mediante fotografías o copias no autorizadas de las carpetas almacenadas en el archivo, empleando dispositivos móviles por falta de control en el acceso al mismo	A.5.1.1 A.6.2.1 A.8.3.1 A.9.1.1	1. Directrices rectorales sobre la conexión de dispositivos ajenos a la IED en los equipos de la Institución
8	Acceso a información confidencial mediante la sustracción de información del computador de la secretaría académica empleando conexión no autorizada a través de dispositivos móviles o unidades de almacenamiento extraíble	A.5.1.1 A.11.1.2	1. Control de acceso de personas externas a la IED mediante personal de seguridad
		A.11.1.1	2, Control de acceso a la IED mediante mallas, muros y cercados

NO RIESGO	ESCENARIO DE RIESGO	COD CTRL	CONTROL ACTUAL
		A.5.1.1 A.6.2.1 A.8.3.1	2. Directrices rectorales sobre la conexión de dispositivos ajenos a la IED en los equipos de la Institución
9	Acceso a información confidencial de los estudiantes a través de dispositivos móviles durante el proceso de registro de calificaciones en el software de la IED, por exposición del escritorio de trabajo de la secretaria académica a personal no autorizado	A.6.2.1 A.8.3.1	1. Directrices rectorales sobre la conexión de dispositivos ajenos a la IED en los equipos de la Institución
10	Acceso a información confidencial mediante la interceptación de la red interna de la secretaría académica a través del cableado del cielo raso que queda expuesto fuera de las oficinas por falta de mecanismos de protección	A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.6	1. Cámaras de vigilancia
		A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.6	2. Sensores de movimiento
		A.11.1.2	3. Control de acceso de personas externas a la IED mediante personal de seguridad
11	Tratamiento erróneo de la información de los estudiantes en el software de control de la IED y/o en el SIMAT afectando los reportes requeridos por la Secretaría de Educación y los informes a la rectoría por falta de entrenamiento del personal	A.12.1.1 A.12.1.2 A.7.2.2	1. Capacitaciones con las entidades correspondientes cuando se llevan a cabo cambios en la plataforma de ingreso de información del Ministerios de Educación Nacional, ICFES (Pruebas Saber PRO) y cuando se presentan cambios del Software Institucional previa aprobación de la Secretaría de Educación.

NO RIESGO	ESCENARIO DE RIESGO	COD CTRL	CONTROL ACTUAL
		A.16.1.2 A.16.1.3	2. Entrega periódica de informes de manera verbal y/o escrita a la rectoría sobre las novedades presentadas en las plataformas de gestión de información empleadas
12	Alteración de la información académica de los estudiantes por errores en el tratamiento de la información por parte del software de control académico de la IED	A.16.1.2 A.16.1.3 A.16.1.5	1. Entrega periódica de informes de manera verbal y/o escrita a la rectoría sobre las novedades presentadas en las plataformas de gestión de información empleadas
13	Alteración del proceso de generación de actas de grado, mediante la expedición errónea y/o no autorizada de actas con sello de la institución con participación del personal de la secretaría académica	A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.6	1. Cámaras de vigilancia
		A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.6	2. Sensores de movimiento
14	Divulgación no autorizada por parte del personal de la secretaría académica de la información de personal de los estudiantes y/o docentes a terceros	A.5.1.1	1. Principio de Ética del Manual de Convivencia de la IED
15	Tratamiento erróneo de la información de los estudiantes y/o docentes tanto digital como física por deficiencias en los canales de comunicación de las políticas administrativas establecidas por el rector de la institución	A.5.1.1	1. Directrices de comunicación establecidos por la rectoría
16	Acceso no autorizado al área de archivo de las carpetas con la información de los estudiantes y/o docentes de la IED, por falta de mecanismos de control de acceso de personal externo	A.11.1.2	1. Control de acceso de personas externas a la IED mediante personal de seguridad
		A.11.1.1	2, Control de acceso a la IED mediante mallas, muros y cercados

NO RIESGO	ESCENARIO DE RIESGO	COD CTRL	CONTROL ACTUAL
		A.11.1.3	3. Ventanas con rejas de hierro para prevenir el acceso no autorizado de terceros
		A.5.1.1 A.9.1.1	4. Políticas rectorales sobre el acceso a la información del archivo por parte de personal no autorizado
		A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.6	5. Cámaras de vigilancia
		A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.6	6. Sensores de movimiento
17	Acceso no autorizado al computador del área de secretaría académica por falta de mecanismos de control de acceso a personal externo y/o falta de control en la atención al público	A.5.1.1 A.11.1.2	1. Control de acceso de personas externas a la IED mediante personal de seguridad
		A.11.1.1	2, Control de acceso a la IED mediante mallas, muros y cercados
		A.11.1.3	3.Ventanas con rejas de hierro para prevenir el acceso no autorizado de terceros
		A.5.1.1 A.9.4.3	4.Protección con contraseñas del equipo de secretaría académica
		A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.6	5.Cámaras de vigilancia

NO RIESGO	ESCENARIO DE RIESGO	COD CTRL	CONTROL ACTUAL
		A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.6	6.Sensores de movimiento
18	Acceso no autorizado al software de control académico por ausencia de mecanismos de control en el puesto de trabajo de la secretaria académica	A.5.1.1 A.11.1.2	1. Control de acceso de personas externas a la IED mediante personal de seguridad
		A.11.1.1	2, Control de acceso a la IED mediante mallas, muros y cercados
		A.11.1.3	3.Ventanas con rejas de hierro para prevenir el acceso no autorizado de terceros
		A.5.1.1 A.9.4.3	4.Protección con contraseñas del equipo de secretaría académica
		A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.6	5.Cámaras de vigilancia
		A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.6	6.Sensores de movimiento
19	Acceso no autorizado al proceso de matrícula de los estudiantes en el software de la IED y/o al SIMAT por ausencia de políticas sobre el manejo confidencial de la información de registro académico	A.5.1.1 A.11.1.2	1. Control de acceso de personas externas a la IED mediante personal de seguridad
		A.11.1.3	2.Ventanas con rejas de hierro para prevenir el acceso no autorizado de terceros
		A.5.1.1 A.9.4.3	3. Protección con contraseñas del equipo de secretaría académica

NO RIESGO	ESCENARIO DE RIESGO	COD CTRL	CONTROL ACTUAL
		A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.6	4. Cámaras de vigilancia
		A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.6	5. Sensores de movimiento
20	Acceso no autorizado al proceso de registro de calificaciones de los estudiantes en el software de la IED por ausencia de políticas sobre el manejo confidencial de la información de registro académico	A.5.1.1 A.11.1.2	1. Control de acceso de personas externas a la IED mediante personal de seguridad
		A.11.1.3	2.Ventanas con rejas de hierro para prevenir el acceso no autorizado de terceros
		A.5.1.1 A.9.4.3	3.Protección con contraseñas del equipo de secretaría académica
		A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.6	4.Cámaras de vigilancia
		A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.6	5.Sensores de movimiento
21	Acceso no autorizado a las plantillas institucionales para la generación de actas de grado por falta de controles para el uso del computador de la secretaría académica	A.11.1.2	1. Control de acceso de personas externas a la IED mediante personal de seguridad
		A.11.1.3	2. Ventanas con rejas de hierro para prevenir el acceso no autorizado de terceros

NO RIESGO	ESCENARIO DE RIESGO	COD CTRL	CONTROL ACTUAL
		A.9.4.3	3. Protección con contraseñas del equipo de secretaría académica
		A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.6	4. Cámaras de vigilancia
		A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.6	5. Sensores de movimiento
22	Acceso no autorizado a información física y/o digital de los estudiantes y docentes por falta de políticas de acceso para personal no autorizado a la Institución y al área de secretaría académica por parte del rector	A.5.1.1 A.9.1.1 A.11.1.2	1. Control de acceso de personas externas a la IED mediante personal de seguridad
		A.11.1.1	2, Control de acceso a la IED mediante mallas, muros y cercados
		A.11.1.3	3.Ventanas con rejas de hierro para prevenir el acceso no autorizado de terceros
		A.5.1.1 A.9.4.3	4.Protección con contraseñas del equipo de secretaría académica
		A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.6	5.Cámaras de vigilancia

NO RIESGO	ESCENARIO DE RIESGO	COD CTRL	CONTROL ACTUAL
		A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.6	6.Sensores de movimiento
23	Acceso a información confidencial física y/o digital de estudiantes y docentes por parte de los ex colaboradores de la institución por falta de controles para la eliminación de usuarios y políticas de acceso a la planta física de personal retirado de la institución	A.5.1.1 A.9.1.1 A.11.1.2	1. Control de acceso de personas externas a la IED mediante personal de seguridad
		A.11.1.1	2, Control de acceso a la IED mediante mallas, muros y cercados
		A.11.1.3	3.Ventanas con rejas de hierro para prevenir el acceso no autorizado de terceros
		A.5.1.1 A.6.2.1 A.9.4.3	4. Protección con contraseñas del equipo de secretaría académica
		A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.6	5. Cámaras de vigilancia
		A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.6	6. Sensores de movimiento
24	Errores en el tratamiento de información por ausencia de entrenamiento y/o instrumentos de consulta que permitan que	A.7.1.2 A.12.1.1	1. Manual de funciones y responsabilidades

NO RIESGO	ESCENARIO DE RIESGO	COD CTRL	CONTROL ACTUAL
	el nuevo personal del área de secretaría académica consulte las particularidades de los procesos adelantados con la información de estudiantes y docentes, tanto en el manejo del archivo físico como en el software de la IED por falta de exigencia de la rectoría en la entrega adecuada del puesto de trabajo por parte de los funcionarios retirados, así como la solicitud de manuales que permitan saber las actividades propias del proceso	A.12.1.1 A.12.1.2 A.7.2.2	2. Capacitaciones con las entidades correspondientes cuando se llevan a cabo cambios en la plataforma de ingreso de información del Ministerios de Educación Nacional, ICFES (Pruebas Saber PRO) y cuando se presentan cambios del Software Institucional previa aprobación de la Secretaría de Educación
25	Hurto de dispositivos de almacenamiento, procesamiento y/o impresoras del área de secretaría académica por falta de controles de acceso a la IED y al área en horarios de atención al público	A.11.1.2	1. Control de acceso de personas externas a la IED mediante personal de seguridad
		A.11.1.1	2, Control de acceso a la IED mediante mallas, muros y cercados
		A.11.1.3	3. Ventanas con rejas de hierro para prevenir el acceso no autorizado de terceros
		A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.6	4. Cámaras de vigilancia
		A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.6	5. Sensores de movimiento

NO RIESGO	ESCENARIO DE RIESGO	COD CTRL	CONTROL ACTUAL
26	Fallos en el equipo de cómputo de la secretaría académica por uso inadecuado del recurso por parte del personal del área	A.12.1.1 A.12.1.2 A.7.2.2	1. Capacitaciones con las entidades correspondientes cuando se llevan a cabo cambios en la plataforma de ingreso de información del Ministerios de Educación Nacional, ICFES (Pruebas Saber PRO) y cuando se presentan cambios del Software Institucional previa aprobación de la Secretaría de Educación.
		A.16.1.2 A.16.1.3 A.16.1.5	2. Entrega periódica de informes de manera verbal y/o escrita a la rectoría sobre las novedades presentadas en las plataformas de gestión de información empleadas
27	Averías en el equipo de cómputo de la secretaría académica por falta de mantenimiento preventivo programado por la rectoría	A.15.1.2 A.15.1.3 A.16.1.5	1. Contratación de proveedor externo para servicios de mantenimiento y atención de incidentes
		A.16.1.2 A.16.1.3	2. Entrega periódica de informes de manera verbal y/o escrita a la rectoría sobre las novedades presentadas en las plataformas de gestión de información empleadas
28	Averías en el equipo de cómputo de la secretaría académica por el no reporte oportuno de las incidencias por parte de la secretaria académica	A.15.1.2 A.15.1.3 A.16.1.5	1. Contratación de proveedor externo para servicios de mantenimiento y atención de incidentes
		A.16.1.2 A.16.1.3	2. Entrega periódica de informes de manera verbal y/o escrita a la rectoría sobre las novedades presentadas en las plataformas de gestión de información empleadas
29	Demora en la atención de los usuarios por problemas de tiempo en el procesamiento de información del equipo de cómputo de la secretaría académica	A.15.1.2 A.15.1.3 A.16.1.5	1. Contratación de proveedor externo para servicios de mantenimiento y atención de incidentes

NO RIESGO	ESCENARIO DE RIESGO	COD CTRL	CONTROL ACTUAL
		A.16.1.2 A.16.1.3	2. Entrega periódica de informes de manera verbal y/o escrita a la rectoría sobre las novedades presentadas en las plataformas de gestión de información empleadas
30	Demora en la atención de los usuarios por problemas relacionados con la idoneidad en el manejo del equipo de cómputo y/o software para el control académico de la IED por parte de la secretaria académica	A.7.1.2 A.12.1.1	1. Manual de funciones y responsabilidades
		A.12.1.1 A.12.1.2 A.7.2.2	2. Capacitaciones con las entidades correspondientes cuando se llevan a cabo cambios en la plataforma de ingreso de información del Ministerios de Educación Nacional, ICFES (Pruebas Saber PRO) y cuando se presentan cambios del Software Institucional previa aprobación de la Secretaría de Educación
31	Demora en el proceso de atención de los usuarios por desconocimiento e idoneidad para adelantar el proceso de matrícula de los estudiantes	A.7.1.2 A.12.1.1	1. Manual de funciones y responsabilidades
		A.12.1.1 A.12.1.2 A.7.2.2	2. Capacitaciones con las entidades correspondientes cuando se llevan a cabo cambios en la plataforma de ingreso de información del Ministerios de Educación Nacional, ICFES (Pruebas Saber PRO) y cuando se presentan cambios del Software Institucional previa aprobación de la Secretaría de Educación
32	Demora en el proceso de atención de los usuarios por retraso en el proceso de ingreso de las calificaciones reportadas por los docentes al sistema de control de la IED por parte de la secretaria académica	A.12.1.1 A.12.1.2 A.7.2.2	1. Capacitaciones con las entidades correspondientes cuando se llevan a cabo cambios en la plataforma de ingreso de información del Ministerios de Educación Nacional, ICFES (Pruebas Saber PRO) y cuando se presentan cambios del Software Institucional previa aprobación de la Secretaría de Educación

NO RIESGO	ESCENARIO DE RIESGO	COD CTRL	CONTROL ACTUAL
33	Demora en el proceso de atención a los usuarios por citaciones a reuniones constantes en horarios habilitados para atención al público por parte del rector	A.5.1.1	1. Políticas rectorales de los horarios establecidos para reuniones generales
34	Entrega de plantillas institucionales a personal no autorizado por parte de la secretaria académica	A.11.1.2	1. Control de acceso de personas externas a la IED mediante personal de seguridad
		A.9.4.3	2. Protección con contraseñas del equipo de secretaría académica
35	Fallos o demoras en la atención del público por afectación de software malicioso en el equipo de cómputo de la secretaría académica	A.15.1.2 A.15.1.3 A.16.1.2 A.16.1.3 A.16.1.5	1. Contratación de proveedor externo para servicios de mantenimiento y atención de incidentes
		A.6.2.1 A.8.3.1 A.12.2.1	2. Instalación de software antivirus por parte de los proveedores de servicios de tecnología e infección por conexión de dispositivos móviles y unidades de almacenamiento extraíble
36	Afectación del equipo de la secretaría académica por software malicioso a causa del uso inadecuado del recurso por parte del personal de la secretaría académica	A.15.1.2 A.15.1.3 A.16.1.2 A.16.1.3 A.16.1.5	1. Contratación de proveedor externo para servicios de mantenimiento y atención de incidentes
		A.6.2.1 A.8.3.1 A.12.2.1	2. Instalación de software antivirus por parte de los proveedores de servicios de tecnología e infección por conexión de dispositivos móviles y unidades de almacenamiento extraíble
37	Afectaciones de las comunicaciones por infección de software malicioso que incide en los drivers de la tarjeta de red del computador de la secretaría académica	A.6.2.1 A.8.3.1 A.12.2.1	1. Instalación de software antivirus por parte de los proveedores de servicios de tecnología e infección por conexión de dispositivos móviles y unidades de almacenamiento extraíble

NO RIESGO	ESCENARIO DE RIESGO	COD CTRL	CONTROL ACTUAL
		A.16.1.2 A.16.1.3 A.16.1.5	2. Entrega periódica de informes de manera verbal y/o escrita a la rectoría sobre las novedades presentadas en las plataformas de gestión de información empleadas
38	Pérdida del archivo físico de los estudiantes y docentes por ocurrencia de desastre natural (terremoto, derrumbe, inundación, etc.)	A.11.1.4	1. Extintores disponibles y habilitados en el área de secretaría académica
39	Pérdida del equipo de cómputo e información digital de la secretaría académica por ocurrencia de desastre natural (terremoto, derrumbe, inundación, etc.)	A.11.1.4	1. Extintores disponibles y habilitados en el área de secretaría académica
40	Pérdida de las comunicaciones para el reporte a la Secretaría de Educación y/o entidades externas por daños en los sistemas de comunicación ocasionados por desastres naturales	A.15.1.2 A.15.1.3 A.16.1.2 A.16.1.3 A.16.1.5	1. Contratación de proveedor externo para servicios de mantenimiento y atención de incidentes
41	Pérdida de información en el equipo de cómputo de la secretaría académica por fallos del fluido eléctrico	A.15.1.2 A.15.1.3 A.16.1.5	1. Contratación de proveedor externo para servicios de mantenimiento y atención de incidentes
42	Daño en el software de control académico por fallos en el fluido eléctrico	A.15.1.2 A.15.1.3 A.16.1.5	1. Contratación de proveedor externo para servicios de mantenimiento y atención de incidentes
43	Parálisis del proceso de matrícula por fallos en el fluido eléctrico		
44	Retrasos en el proceso de ingreso de calificaciones por fallos en el fluido eléctrico		
45	Daño en el archivo y/o equipos de cómputo e información digital por fuego provocado	A.11.1.4	1. Extintores disponibles y habilitados en el área de secretaría académica

NO RIESGO	ESCENARIO DE RIESGO	COD CTRL	CONTROL ACTUAL
46	Afectación física en el personal del área de secretaría académica por fuego provocado y ausencia de planes de emergencia y/o rutas adecuadas de evacuación	A.11.1.4	1. Extintores disponibles y habilitados en el área de secretaría académica
			2. Señalización de rutas de evacuación
47	Deterioro del archivo físico de los estudiantes y los docentes por corrosión provocada por humedad	A.11.1.4 A.15.1.2 A.15.1.3 A.16.1.5	1. Contratación de proveedores para mantenimiento de la infraestructura física
48	Incumplimiento en los reportes al SIMAT, a la plataforma del ICFES para las pruebas SABER y Secretaría de Educación por fallos en los dispositivos que permiten la prestación del servicio de Internet	A.15.1.2 A.15.1.3 A.16.1.5	1. Contratación de proveedor externo para servicios de mantenimiento y atención de incidentes
		A.12.2.1	2. Instalación de software antivirus por parte de los proveedores de servicios de tecnología
49	Interceptación de datos de los estudiantes por infección con software espía por deficiencias en los mecanismos de protección tales como antivirus y antimalware	A.15.1.2 A.15.1.3 A.16.1.2 A.16.1.3 A.16.1.5	1. Contratación de proveedor externo para servicios de mantenimiento y atención de incidentes
		A.12.2.1	2. Instalación de software antivirus por parte de los proveedores de servicios de tecnología
50	Divulgación de la información de los estudiantes y/o docentes por medio de la práctica inadecuada de desecho de información reciclada por parte de la secretaria académica		
51	Divulgación de la información de los estudiantes y/o docentes por falta de políticas y mecanismos para la adecuada disposición de los desechos		

NO RIESGO	ESCENARIO DE RIESGO	COD CTRL	CONTROL ACTUAL
52	Fallos en el funcionamiento del equipo de cómputo de la secretaría académica por instalación de software pirata, ocasionado por falta de políticas con los proveedores, y el personal de la IED	A.15.1.2 A.15.1.3 A.16.1.5	1. Contratación de proveedor externo para servicios de mantenimiento y atención de incidentes
		A.16.1.2 A.16.1.3	2. Entrega periódica de informes de manera verbal y/o escrita a la rectoría sobre las novedades presentadas en las plataformas de gestión de información empleadas
53	Divulgación y daño en la información confidencial de los estudiantes y/o docentes por retaliaciones políticas en periodos de elecciones por falta de políticas de confidencialidad		
54	Exposición de las contraseñas de acceso a los equipos de cómputo y sistemas de información por falta de medidas de prevención, uso adecuado y preservación de las mismas	A.5.1.1 A.9.1.1	1. Políticas rectorales sobre el acceso de estudiantes al área de archivo
		A.5.1.1 A.9.1.1	2. Políticas rectorales sobre el uso del equipo de cómputo de la secretaría académica por parte de personal no autorizado
55	Demora en el restablecimiento del servicio por fallos relacionados a la extracción de copias de seguridad y pruebas de las mismas	A.15.1.2 A.15.1.3 A.16.1.5	1. Contratación de proveedor externo para servicios de mantenimiento y atención de incidentes

4.1.3.12. Paso 12: Vulnerabilidad residual

Para hallar la vulnerabilidad residual se tienen en cuenta los controles asociados a cada riesgo, modificando el valor inherente de la probabilidad o el impacto, finalmente se suman la totalidad los valores asignados.

$$I_{Total} = I_c + I_i + I_d$$

Donde:

ITotal = Impacto total

Ic = Calificación impacto en la confidencialidad

Ii = Calificación de impacto en la integridad

Id = Calificación de impacto en la disponibilidad

Para calcular la vulnerabilidad residual:

Determine la vulnerabilidad en cada uno de los factores como:

$$V_{Rc} = (P \times I_c)/M_{ax}(P \times I_c)$$

Donde:

VRc = Vulnerabilidad residual Confidencialidad

Ic = Calificación impacto en la confidencialidad

P = Probabilidad

Max(P X Ic) = Máximo valor posible de la probabilidad por el impacto, en esta metodología el máximo valor de la probabilidad es 3, y el máximo valor del impacto es 3, por tanto el denominador de la anterior ecuación es 9.

De igual manera se procede con los otros dos factores.

El cálculo de la vulnerabilidad residual total se halla de:

$$V \quad = (P \times (I_{\iota} + I_{\imath} + I_{\iota}) \div M \quad (P \times (I_{\iota} + I_{\imath} + I_{\iota}))$$

Donde:

VRt = Vulnerabilidad residual total

$M \quad (P \times (I_{\iota} + I_{\imath} + I_{\iota}))$ = Máximo valor posible de la probabilidad por el impacto, en esta metodología el máximo valor de la probabilidad es 3, y el máximo valor de la combinación de los impactos es 9, por tanto, el denominador de la anterior ecuación es 27.

La vulnerabilidad residual se muestra en la siguiente tabla.

Tabla 20. Vulnerabilidad residual – Secretaría Académica IED's

NO	ESCENARIO DE RIESGO	PROBABILIDAD	IMPACTO				VULNERABILIDAD RESIDUAL			
			C	I	D	TOTAL	C	I	D	TOTAL
1	Afectación legal por pérdida de información del computador de la Secretaría Académica de la IED que almacena la información de los estudiantes y contiene los registros y formatos de las actas de grado y certificados de estudio	1	3	3	2	8	33%	33%	22%	30%
2	Afectación legal por pérdida de la información de los estudiantes y/o docentes por deficiencias en los procesos de inducción y capacitación de la Secretaria Académica de la institución	1	3	2	2	7	33%	22%	22%	26%
3	Afectación legal por pérdida mediante sustracción de las carpetas que contienen los soportes académicos de los estudiantes	1	3	3	3	9	33%	33%	33%	33%

NO	ESCENARIO DE RIESGO	PROBABILIDAD	IMPACTO				VULNERABILIDAD RESIDUAL			
			C	I	D	TOTAL	C	I	D	TOTAL
4	Afectación legal por pérdida mediante sustracción de las carpetas que contienen los soportes de cualificación profesional de los docentes	1	3	3	3	9	33%	33%	33%	33%
5	Afectación legal por pérdida de la información del software de control académico de la Institución	2	1	2	3	6	22%	44%	67%	44%
6	Afectación legal por errores en el proceso de matrícula al registrar la información de los estudiantes en el software de la IED y /o en el SIMAT, por parte de personal no idóneo o con falta de entrenamiento	1	1	3	1	5	11%	33%	11%	19%
7	Acceso a información confidencial de los estudiantes y/o docentes mediante fotografías o copias no autorizadas de las carpetas almacenadas en el archivo, empleando dispositivos móviles por falta de control en el acceso al mismo	2	3	1	1	5	67%	22%	22%	37%
8	Acceso a información confidencial mediante la sustracción de información del computador de la secretaría académica empleando conexión no autorizada a través de dispositivos móviles o unidades de almacenamiento extraíble	1	3	3	1	7	33%	33%	11%	26%
9	Acceso a información confidencial de los estudiantes a través de dispositivos móviles durante el proceso de registro de calificaciones en el software de la IED, por exposición del escritorio de trabajo de la	1	1	1	2	4	11%	11%	22%	15%

NO	ESCENARIO DE RIESGO	PROBABILIDAD	IMPACTO				VULNERABILIDAD RESIDUAL			
			C	I	D	TOTAL	C	I	D	TOTAL
	secretaria académica a personal no autorizado									
10	Acceso a información confidencial mediante la interceptación de la red interna de la secretaría académica a través del cableado del cielo raso que queda expuesto fuera de las oficinas por falta de mecanismos de protección	1	3	3	2	8	33%	33%	22%	30%
11	Tratamiento erróneo de la información de los estudiantes en el software de control de la IED y/o en el SIMAT afectando los reportes requeridos por la Secretaría de Educación y los informes a la rectoría por falta de entrenamiento del personal	1	1	3	2	6	11%	33%	22%	22%
12	Alteración de la información académica de los estudiantes por errores en el tratamiento de la información por parte del software de control académico de la IED	1	2	3	2	7	22%	33%	22%	26%
13	Alteración del proceso de generación de actas de grado, mediante la expedición errónea y/o no autorizada de actas con sello de la institución con participación del personal de la secretaría académica	1	2	3	1	6	22%	33%	11%	22%
14	Divulgación no autorizada por parte del personal de la secretaría académica de la información de personal de los estudiantes y/o docentes a terceros	2	3	1	1	5	67%	22%	22%	37%
15	Tratamiento erróneo de la información de los estudiantes y/o docentes tanto digital como física por deficiencias en los canales de comunicación de las políticas	2	1	2	1	4	22%	44%	22%	30%

NO	ESCENARIO DE RIESGO	PROBABILIDAD	IMPACTO				VULNERABILIDAD RESIDUAL			
			C	I	D	TOTAL	C	I	D	TOTAL
	administrativas establecidas por el rector de la institución									
16	Acceso no autorizado al área de archivo de las carpetas con la información de los estudiantes y/o docentes de la IED, por falta de mecanismos de control de acceso de personal externo	1	3	3	3	9	33%	33%	33%	33%
17	Acceso no autorizado al computador del área de secretaría académica por falta de mecanismos de control de acceso a personal externo y/o falta de control en la atención al público	1	3	3	3	9	33%	33%	33%	33%
18	Acceso no autorizado al software de control académico por ausencia de mecanismos de control en el puesto de trabajo de la secretaria académica	2	3	3	3	9	67%	67%	67%	67%
19	Acceso no autorizado al proceso de matrícula de los estudiantes en el software de la IED y/o al SIMAT por ausencia de políticas sobre el manejo confidencial de la información de registro académico	1	3	3	3	9	33%	33%	33%	33%
20	Acceso no autorizado al proceso de registro de calificaciones de los estudiantes en el software de la IED por ausencia de políticas sobre el manejo confidencial de la información de registro académico	1	3	3	3	9	33%	33%	33%	33%
21	Acceso no autorizado a las plantillas institucionales para la generación de actas de grado por falta de controles para el uso del computador de la secretaría académica	1	1	1	1	3	11%	11%	11%	11%

NO	ESCENARIO DE RIESGO	PROBABILIDAD	IMPACTO				VULNERABILIDAD RESIDUAL			
			C	I	D	TOTAL	C	I	D	TOTAL
22	Acceso no autorizado a información física y/o digital de los estudiantes y docentes por falta de políticas de acceso para personal no autorizado a la Institución y al área de secretaría académica por parte del rector	1	3	3	3	9	33%	33%	33%	33%
23	Acceso a información confidencial física y/o digital de estudiantes y docentes por parte de los excolaboradores de la institución por falta de controles para la eliminación de usuarios y políticas de acceso a la planta física de personal retirado de la institución	2	3	3	3	9	67%	67%	67%	67%
24	Errores en el tratamiento de información por ausencia de entrenamiento y/o instrumentos de consulta que permitan que el nuevo personal del área de secretaría académica consulte las particularidades de los procesos adelantados con la información de estudiantes y docentes, tanto en el manejo del archivo físico como en el software de la IED por falta de exigencia de la rectoría en la entrega adecuada del puesto de trabajo por parte de los funcionarios retirados, así como la solicitud de manuales que permitan saber las actividades propias del proceso	3	2	3	2	7	67%	100%	67%	78%
25	Hurto de dispositivos de almacenamiento, procesamiento y/o impresoras del área de secretaría académica por falta de controles de acceso a la IED y al área	1	3	1	2	6	33%	11%	22%	22%

NO	ESCENARIO DE RIESGO	PROBABILIDAD	IMPACTO				VULNERABILIDAD RESIDUAL			
			C	I	D	TOTAL	C	I	D	TOTAL
	en horarios de atención al público									
26	Fallos en el equipo de cómputo de la secretaría académica por uso inadecuado del recurso por parte del personal del área	1	1	3	3	7	11%	33%	33%	26%
27	Averías en el equipo de cómputo de la secretaría académica por falta de mantenimiento preventivo programado por la rectoría	1	1	3	3	7	11%	33%	33%	26%
28	Averías en el equipo de cómputo de la secretaría académica por el no reporte oportuno de las incidencias por parte de la secretaria académica	1	1	3	3	7	11%	33%	33%	26%
29	Demora en la atención de los usuarios por problemas de tiempo en el procesamiento de información del equipo de cómputo de la secretaría académica	2	1	1	3	5	22%	22%	67%	37%
30	Demora en la atención de los usuarios por problemas relacionados con la idoneidad en el manejo del equipo de cómputo y/o software para el control académico de la IED por parte de la secretaria académica	2	1	1	3	5	22%	22%	67%	37%
31	Demora en el proceso de atención de los usuarios por desconocimiento e idoneidad para adelantar el proceso de matrícula de los estudiantes	1	1	1	3	5	11%	11%	33%	19%
32	Demora en el proceso de atención de los usuarios por retraso en el proceso de ingreso de las calificaciones reportadas por los docentes al sistema de control de la IED por parte de la secretaria académica	2	1	1	3	5	22%	22%	67%	37%

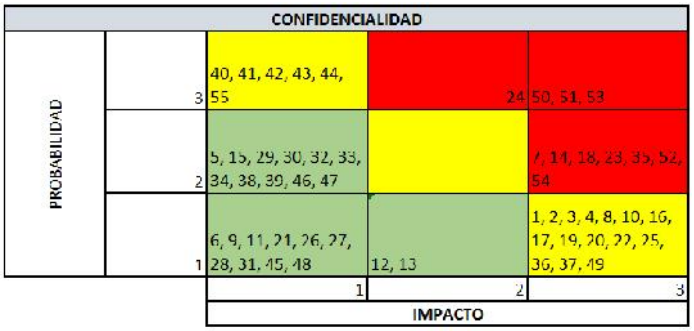
NO	ESCENARIO DE RIESGO	PROBABILIDAD	IMPACTO				VULNERABILIDAD RESIDUAL			
			C	I	D	TOTAL	C	I	D	TOTAL
33	Demora en el proceso de atención a los usuarios por citaciones a reuniones constantes en horarios habilitados para atención al público por parte del rector	2	1	1	3	5	22%	22%	67%	37%
34	Entrega de plantillas institucionales a personal no autorizado por parte de la secretaria académica	2	1	1	1	3	22%	22%	22%	22%
35	Fallos o demoras en la atención del público por afectación de software malicioso en el equipo de cómputo de la secretaría académica	2	3	3	3	9	67%	67%	67%	67%
36	Afectación del equipo de la secretaría académica por software malicioso a causa del uso inadecuado del recurso por parte del personal de la secretaría académica	1	3	3	3	9	33%	33%	33%	33%
37	Afectaciones de las comunicaciones por infección de software malicioso que incide en los drivers de la tarjeta de red del computador de la secretaría académica	1	3	3	3	9	33%	33%	33%	33%
38	Pérdida del archivo físico de los estudiantes y docentes por ocurrencia de desastre natural (terremoto, derrumbe, inundación, etc.)	2	1	2	2	5	22%	44%	44%	37%
39	Pérdida del equipo de cómputo e información digital de la secretaría académica por ocurrencia de desastre natural (terremoto, derrumbe, inundación, etc.)	2	1	2	2	5	22%	44%	44%	37%
40	Pérdida de las comunicaciones para el reporte a la Secretaría de Educación y/o entidades externas por daños en los sistemas de comunicación ocasionados por desastres naturales	3	1	1	2	4	33%	33%	67%	44%

NO	ESCENARIO DE RIESGO	PROBABILIDAD	IMPACTO				VULNERABILIDAD RESIDUAL			
			C	I	D	TOTAL	C	I	D	TOTAL
41	Pérdida de información en el equipo de cómputo de la secretaría académica por fallos del fluido electríco	3	1	3	2	6	33%	100%	67%	67%
42	Daño en el software de control académico por fallos en el fluído eléctrico	3	1	3	2	6	33%	100%	67%	67%
43	Parálisis del proceso de matrícula por fallos en el fluído eléctrico	3	1	1	3	5	33%	33%	100%	56%
44	Retrasos en el proceso de ingreso de calificaciones por fallos en el fluído eléctrico	3	1	1	3	5	33%	33%	100%	56%
45	Daño en el archivo y/o equipos de cómputo e información digital por fuego provocado	1	1	2	2	5	11%	22%	22%	19%
46	Afectación física en el personal del área de secretaría académica por fuego provocado y ausencia de planes de emergencia y/o rutas adecuadas de evacuación	2	1	1	2	4	22%	22%	44%	30%
47	Deterioro del archivo físico de los estudiantes y los docentes por corrosión provocada por humedad	2	1	3	3	7	22%	67%	67%	52%
48	Incumplimiento en los reportes al SIMAT, a la plataforma del ICFES para las pruebas SABER y Secretaría de Educación por fallos en los dispositivos que permiten la prestación del servicio de Internet	1	1	1	3	5	11%	11%	33%	19%
49	Interceptación de datos de los estudiantes por infección con software espia por deficiencias en los mecanismos de protección tales como antivirus y antimalware	1	3	3	3	9	33%	33%	33%	33%
50	Divulgación de la información de los estudiantes y/o docentes por medio de la práctica inadecuada de desecho de	3	3	1	1	5	100%	33%	33%	56%

NO	ESCENARIO DE RIESGO	PROBABILIDAD	IMPACTO				VULNERABILIDAD RESIDUAL			
			C	I	D	TOTAL	C	I	D	TOTAL
	información reciclada por parte de la secretaria académica									
51	Divulgación de la información de los estudiantes y/o docentes por falta de políticas y mecanismos para la adecuada disposición de los desechos	3	3	1	1	5	100%	33%	33%	56%
52	Fallos en el funcionamiento del equipo de cómputo de la secretaría académica por instalación de software pirata, ocasionado por falta de políticas con los proveedores, y el personal de la IED	2	3	3	3	9	67%	67%	67%	67%
53	Divulgación y daño en la información confidencial de los estudiantes y/o docentes por retaliaciones políticas en periodos de elecciones por falta de políticas de confidencialidad	3	3	3	3	9	100%	100%	100%	100%
54	Exposición de las contraseñas de acceso a los equipos de cómputo y sistemas de información por falta de medidas de prevención, uso adecuado y preservación de las mismas	2	3	3	3	9	67%	67%	67%	67%
55	Demora en el restablecimiento del servicio por fallos relacionados a la extracción de copias de seguridad y pruebas de las mismas	3	1	3	3	7	33%	100%	100%	78%

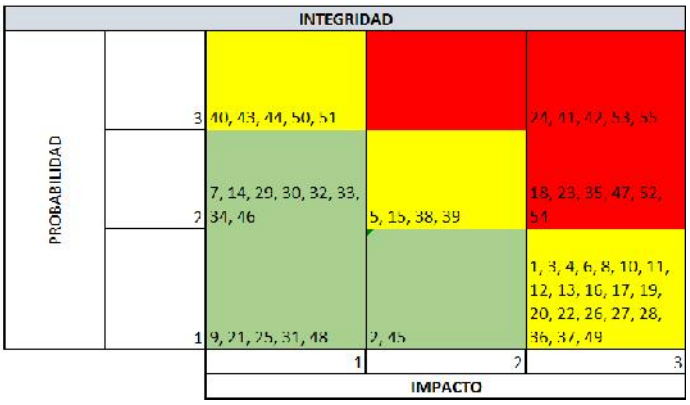
4.1.3.13. Paso 13: Mapas de temperatura de vulnerabilidad residual

Las gráficas 50, 51, 52, 53 y 54 ubican los valores resultantes de la calificación de la vulnerabilidad residual, teniendo en cuenta los controles del anexo A de la Norma NTC ISO/IEC 27001:2013.



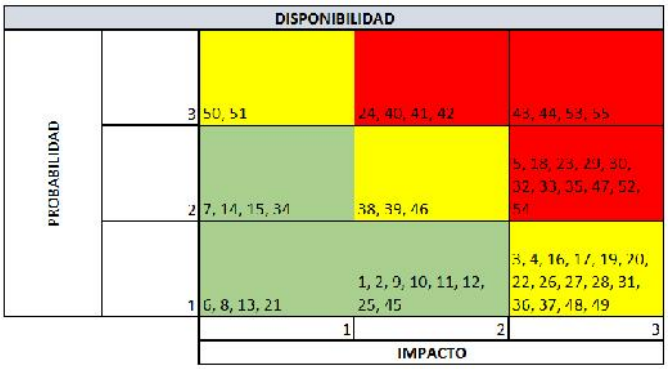
Gráfica 50. Vulnerabilidad residual confidencialidad

Fuente: propia



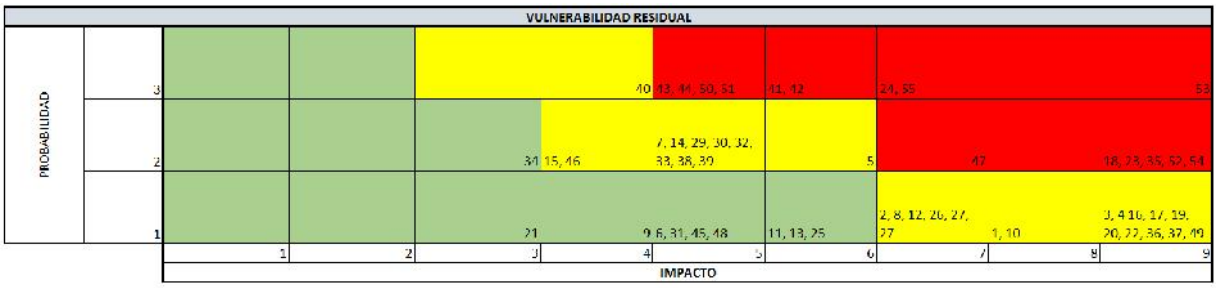
Gráfica 51. Vulnerabilidad residual integridad

Fuente: propia



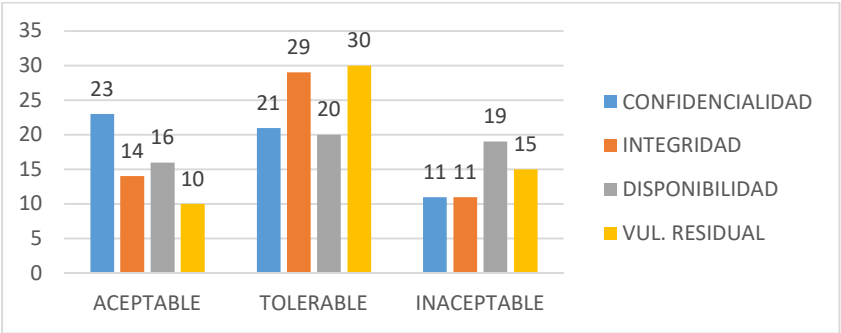
Gráfica 52. Vulnerabilidad residual disponibilidad

Fuente: propia



Gráfica 53. Vulnerabilidad residual total

Fuente: propia



Gráfica 54. Cantidad de riesgos por criterio y por aceptabilidad en el análisis de la vulnerabilidad residual

Fuente: propia

4.1.3.14. Paso 14: Plan de tratamiento de riesgos

N.	ESCENARIO DE RIESGO	PLAN DE MITIGACIÓN DE RIESGOS					
		ESTRATEGIA	ACTIVIDAD	RESPONSABLE	VALOR	FECHA INICIO	FECHA FINAL
1	Afectación legal por pérdida de información del computador de la Secretaría Académica de la IED que almacena la información de los estudiantes y contiene los registros y formatos de las actas de grado y certificados de estudio	Concientizar al personal de la secretaría académica sobre la importancia de preservar adecuadamente la información de los niños, niñas, adolescentes y docentes	Establecer un cronograma de capacitaciones sobre la Ley 1581/2012 y las disposiciones del MEN en términos de protección de la información de los estudiantes y docentes	Rector		15/01/18	30/11/18
		Establecer directrices para garantizar que la información de los estudiantes y docentes no es evidente a simple vista por personal no autorizado en las zonas de atención al público	Definir protocolos de seguridad cuando el equipo de cómputo se encuentra desatendido	Rector		15/01/18	30/11/18
			Definir protocolos de prevención de exposición de la información en el escritorio de la secretaría académica	Rector		15/01/18	30/11/18
		Establecer procedimientos documentados para el adecuado manejo de las claves de acceso al equipo de cómputo y a los Sistemas de Información	Definir protocolos de manejo adecuado de claves	Rector		15/01/18	30/11/18
		Establecer procedimientos de copia de seguridad	Definir protocolos para generar copias de seguridad	Rector		15/01/18	30/11/18
2	Afectación legal por pérdida de la información de los estudiantes y/o docentes por deficiencias en los procesos de inducción y capacitación de la Secretaria	Controlar adecuadamente la efectividad de los procesos de inducción	Establecer mecanismos que permitan verificar la efectividad de los procesos de inducción	Rector		15/01/18	30/11/18
			Establecer cronograma de reinducciones periódicas, teniendo en cuenta los resultados arrojados en la evaluación de la efectividad de la inducción	Rector		15/01/18	30/11/18

N.	ESCENARIO DE RIESGO	PLAN DE MITIGACIÓN DE RIESGOS					
		ESTRATEGIA	ACTIVIDAD	RESPONSABLE	VALOR	FECHA INICIO	FECHA FINAL
	Académica de la institución	Establecer mecanismos para medir el desempeño de los funcionarios	Definir las competencias laborales y comportamentales a ser incluidas en la evaluación de desempeño relacionada con el tratamiento de la información	Rector		15/01/18	30/11/18
3	Afectación legal por pérdida mediante sustracción de las carpetas que contienen los soportes académicos de los estudiantes	Identificar la información crítica almacenada en el área de archivo y establecer, mantener y controlar mecanismos que permitan impedir el intento de sustracción	Caracterizar la información crítica del archivo	Rector		15/01/18	30/11/18
			Establecer políticas para el manejo de llaves del archivo y de las puertas de acceso al mismo				
4	Afectación legal por pérdida mediante sustracción de las carpetas que contienen los soportes de cualificación profesional de los docentes		Establecer políticas sobre el acceso restringido de personal al área de archivo cuando se atiende público externo				
5	Afectación legal por pérdida de la información del software de control académico de la Institución	Concientizar al personal de la secretaría académica sobre la importancia de preservar adecuadamente la información de los niños, niñas, adolescentes y docentes	Establecer un cronograma de capacitaciones sobre la Ley 1581/2012 y las disposiciones del MEN en términos de protección de la información de los estudiantes y docentes	Rector		15/01/18	30/11/18
		Establecer procedimientos documentados para el adecuado manejo de las claves de acceso al equipo de cómputo y a los Sistemas de Información	Definir protocolos de manejo adecuado de claves	Rector		15/01/18	30/11/18
		Establecer procedimientos de copia de seguridad	Definir protocolos para generar copias de seguridad	Rector		15/01/18	30/11/18

N.	ESCENARIO DE RIESGO	PLAN DE MITIGACIÓN DE RIESGOS					
		ESTRATEGIA	ACTIVIDAD	RESPONSABLE	VALOR	FECHA INICIO	FECHA FINAL
7	Acceso a información confidencial de los estudiantes y/o docentes mediante fotografías o copias no autorizadas de las carpetas almacenadas en el archivo, empleando dispositivos móviles por falta de control en el acceso al mismo	Establecer políticas para el manejo adecuado de dispositivos móviles en el área de archivo de la secretaría académica	Revisar y complementar las disposiciones rectorales sobre el manejo de dispositivos móviles en el área de archivo	Rector		15/01/18	30/11/18
		Identificar la información crítica almacenada en el área de archivo y establecer, mantener y controlar mecanismos que permitan impedir el intento de sustracción	Caracterizar la información crítica del archivo	Rector		15/01/18	30/11/18
			Establecer políticas para el manejo de llaves del archivo y de las puertas de acceso al mismo	Rector		15/01/18	30/11/18
			Establecer políticas sobre el acceso restringido de personal al área de archivo cuando se atiende público externo	Rector		15/01/18	30/11/18
8	Acceso a información confidencial mediante la sustracción de información del computador de la secretaría académica empleando conexión no autorizada a través de dispositivos móviles o unidades de almacenamiento extraíble	Establecer procedimientos documentados para el adecuado manejo de las claves de acceso al equipo de cómputo y a los Sistemas de Información	Definir protocolos de manejo adecuado de claves	Rector		15/01/18	30/11/18
		Establecer políticas para el manejo adecuado de dispositivos móviles y unidades de almacenamiento extraíble en el área de archivo de la secretaría académica	Revisar y complementar las disposiciones rectorales sobre el manejo de dispositivos móviles y unidades de almacenamiento extraíbles en el área de archivo	Rector		15/01/18	30/11/18
10	Acceso a información confidencial mediante la interceptación de la red interna de la secretaría académica a través del cableado del cielo raso que queda expuesto fuera de las oficinas por falta de	Establecer medidas complementarias para la disuasión de intrusos a través del techo de la IED	Implementar luces reflectoras que iluminen la zona perimetral de la secretaría académica	Rector		15/01/18	30/11/18
		Revisar el tendido de cableado que pasa por el cielo raso, distribuyéndolo adecuadamente	Organizar el cableado de red de la secretaría académica, identificando adecuadamente su trayectoria	Rector		15/01/18	30/11/18

N.	ESCENARIO DE RIESGO	PLAN DE MITIGACIÓN DE RIESGOS					
		ESTRATEGIA	ACTIVIDAD	RESPONSABLE	VALOR	FECHA INICIO	FECHA FINAL
	mecanismos de protección	y empleando los medios apropiados	Instalar canaleta para el cableado de red de la secretaría académica	Rector		15/01/18	30/11/18
12	Alteración de la información académica de los estudiantes por errores en el tratamiento de la información por parte del software de control académico de la IED	Establecer medidas que permitan garantizar el adecuado funcionamiento de los sistemas de información de la secretaría académica	Elaborar cronogramas de mantenimiento preventivo de los equipos de cómputo	Rector		15/01/18	30/11/18
		Establecer mecanismos de comunicación efectivos para la detección y atención oportuna de los incidentes presentados en los sistemas de información	Definir protocolos adecuados para la comunicación de incidentes, permitiendo su trazabilidad	Rector		15/01/18	30/11/18
		Revisar la oportunidad de atención de los proveedores de servicios de tecnología	Establecer acuerdos de oportuna atención con los proveedores encargados de brindar soporte a los sistemas de información	Rector		15/01/18	30/11/18
14	Divulgación no autorizada por parte del personal de la secretaría académica de la información de personal de los estudiantes y/o docentes a terceros	Establecer mecanismos que permitan preservar la información confidencial	Definir acuerdos de confidencialidad con los funcionarios del área de secretaría académica	Rector		15/01/18	30/11/18
		Concientizar al personal de la secretaría académica sobre la importancia de preservar adecuadamente la información de los niños, niñas, adolescentes y docentes	Establecer un cronograma de capacitaciones sobre la Ley 1581/2012 y las disposiciones del MEN en términos de protección de la información de los estudiantes y docentes	Rector		15/01/18	30/11/18
15	Tratamiento erróneo de la información de los estudiantes y/o docentes tanto digital como física por deficiencias en los canales de comunicación	Controlar adecuadamente la efectividad de los procesos de inducción	Establecer mecanismos que permitan verificar la efectividad de los procesos de inducción	Rector		15/01/18	30/11/18
			Establecer cronograma de reinducciones periódicas, teniendo en cuenta los resultados	Rector		15/01/18	30/11/18

N.	ESCENARIO DE RIESGO	PLAN DE MITIGACIÓN DE RIESGOS					
		ESTRATEGIA	ACTIVIDAD	RESPONSABLE	VALOR	FECHA INICIO	FECHA FINAL
	de las políticas administrativas establecidas por el rector de la institución		arrojados en la evaluación de la efectividad de la inducción				
		Definir mecanismos de comunicación tanto internos como externos	Establecer un protocolo de comunicación tanto de las políticas internas como de la información relevante hacia el interior de la IED y hacia el exterior de la misma	Rector		15/01/18	30/11/18
16	Acceso no autorizado al área de archivo de las carpetas con la información de los estudiantes y/o docentes de la IED, por falta de mecanismos de control de acceso de personal externo	Identificar la información crítica almacenada en el área de archivo y establecer, mantener y controlar mecanismos que permitan impedir el intento de sustracción	Caracterizar la información crítica del archivo	Rector		15/01/18	30/11/18
			Establecer políticas para el manejo de llaves del archivo y de las puertas de acceso al mismo	Rector		15/01/18	30/11/18
			Establecer políticas sobre el acceso restringido de personal al área de archivo cuando se atiende público externo	Rector		15/01/18	30/11/18
17	Acceso no autorizado al computador del área de secretaría académica por falta de mecanismos de control de acceso a personal externo y/o falta de control en la atención al público	Establecer directrices para garantizar que la información de los estudiantes y docentes no es evidente a simple vista por personal no autorizado en las zonas de atención al público	Definir protocolos de seguridad cuando el equipo de cómputo se encuentra desatendido	Rector		15/01/18	30/11/18
18	Acceso no autorizado al software de control académico por ausencia de mecanismos de control en el puesto de trabajo de la secretaria académica		Definir protocolos de prevención de exposición de la información en el escritorio de la secretaría académica				
		Establecer procedimientos documentados para el adecuado manejo de las claves de acceso	Definir protocolos de manejo adecuado de claves				

N.	ESCENARIO DE RIESGO	PLAN DE MITIGACIÓN DE RIESGOS					
		ESTRATEGIA	ACTIVIDAD	RESPONSABLE	VALOR	FECHA INICIO	FECHA FINAL
19	Acceso no autorizado al proceso de matrícula de los estudiantes en el software de la IED y/o al SIMAT por ausencia de políticas sobre el manejo confidencial de la información de registro académico	al equipo de cómputo y a los Sistemas de Información					
20	Acceso no autorizado al proceso de registro de calificaciones de los estudiantes en el software de la IED por ausencia de políticas sobre el manejo confidencial de la información de registro académico						
22	Acceso no autorizado a información física y/o digital de los estudiantes y docentes por falta de políticas de acceso para personal no autorizado a la Institución y al área de secretaría académica por parte del rector	Establecer directrices para garantizar que la información de los estudiantes y docentes no es evidente a simple vista por personal no autorizado en las zonas de atención al público	Definir protocolos de seguridad cuando el equipo de cómputo se encuentra desatendido	Rector		15/01/18	30/11/18
			Definir protocolos de prevención de exposición de la información en el escritorio de la secretaría académica	Rector		15/01/18	30/11/18
		Establecer procedimientos documentados para el adecuado manejo de las claves de acceso al equipo de cómputo y a los Sistemas de Información	Definir protocolos de manejo adecuado de claves	Rector		15/01/18	30/11/18
		Identificar la información crítica almacenada en el área de	Caracterizar la información crítica del archivo	Rector		15/01/18	30/11/18

N.	ESCENARIO DE RIESGO	PLAN DE MITIGACIÓN DE RIESGOS					
		ESTRATEGIA	ACTIVIDAD	RESPONSABLE	VALOR	FECHA INICIO	FECHA FINAL
		archivo y establecer, mantener y controlar mecanismos que permitan impedir el intento de sustracción	Establecer políticas para el manejo de llaves del archivo y de las puertas de acceso al mismo	Rector		15/01/18	30/11/18
			Establecer políticas sobre el acceso restringido de personal al área de archivo cuando se atiende público externo	Rector		15/01/18	30/11/18
23	Acceso a información confidencial física y/o digital de estudiantes y docentes por parte de los ex colaboradores de la institución por falta de controles para la eliminación de usuarios y políticas de acceso a la planta física de personal retirado de la institución	Establecer directrices para garantizar que la información de los estudiantes y docentes no es evidente a simple vista por personal no autorizado en las zonas de atención al público	Definir protocolos de seguridad cuando el equipo de cómputo se encuentra desatendido	Rector		15/01/18	30/11/18
			Definir protocolos de prevención de exposición de la información en el escritorio de la secretaría académica	Rector		15/01/18	30/11/18
		Establecer procedimientos documentados para el adecuado manejo de las claves de acceso al equipo de cómputo y a los Sistemas de Información	Definir protocolos de manejo adecuado de claves	Rector		15/01/18	30/11/18
		Identificar la información crítica almacenada en el área de archivo y establecer, mantener y controlar mecanismos que permitan impedir el intento de sustracción	Caracterizar la información crítica del archivo	Rector		15/01/18	30/11/18
			Establecer políticas para el manejo de llaves del archivo y de las puertas de acceso al mismo	Rector		15/01/18	30/11/18
			Establecer políticas sobre el acceso restringido de personal al área de archivo cuando se atiende público externo	Rector		15/01/18	30/11/18
		Establecer políticas para el manejo adecuado de dispositivos móviles en el área de archivo de la secretaría académica	Revisar y complementar las disposiciones rectorales sobre el manejo de dispositivos móviles en el área de archivo	Rector		15/01/18	30/11/18

N.	ESCENARIO DE RIESGO	PLAN DE MITIGACIÓN DE RIESGOS					
		ESTRATEGIA	ACTIVIDAD	RESPONSABLE	VALOR	FECHA INICIO	FECHA FINAL
		Revisar la política de control de acceso de personal externo a la IED	Establecer una política de control de acceso a la IED que tenga en cuenta los permisos de acceso de los exfuncionarios	Rector		15/01/18	30/11/18
24	Errores en el tratamiento de información por ausencia de entrenamiento y/o instrumentos de consulta que permitan que el nuevo personal del área de secretaría académica consulte las particularidades de los procesos adelantados con la información de estudiantes y docentes, tanto en el manejo del archivo físico como en el software de la IED por falta de exigencia de la rectoría en la entrega adecuada del puesto de trabajo por parte de los funcionarios retirados, así como la solicitud de manuales que permitan saber las actividades propias del proceso	Controlar adecuadamente la efectividad de los procesos de inducción	Establecer mecanismos que permitan verificar la efectividad de los procesos de inducción	Rector		15/01/18	30/11/18
			Establecer cronograma de reinducciones periódicas, teniendo en cuenta los resultados arrojados en la evaluación de la efectividad de la inducción	Rector		15/01/18	30/11/18
		Revisar los requisitos establecidos para la entrega del cargo	Definir protocolos para la entrega adecuada del cargo cuando el funcionario es removido o trasladado de IED	Rector		15/01/18	30/11/18
		Establecer mecanismos para medir el desempeño de los funcionarios	Definir las competencias laborales y comportamentales a ser incluidas en la evaluación de desempeño relacionada con el tratamiento de la información	Rector		15/01/18	30/11/18
26	Fallos en el equipo de cómputo de la secretaría académica por uso inadecuado del recurso	Establecer mecanismos de comunicación efectivos para la detección y atención oportuna	Definir protocolos adecuados para la comunicación de incidentes, permitiendo su trazabilidad	Rector		15/01/18	30/11/18

N.	ESCENARIO DE RIESGO	PLAN DE MITIGACIÓN DE RIESGOS					
		ESTRATEGIA	ACTIVIDAD	RESPONSABLE	VALOR	FECHA INICIO	FECHA FINAL
	por parte del personal del área	de los incidentes presentados en los sistemas de información					
		Definir mecanismos que permitan el uso adecuado de los recursos tecnológicos del área de secretaría académica	Establecer un plan de capacitación anual para el uso adecuado de los recursos tecnológicos	Rector		15/01/18	30/11/18
27	Averías en el equipo de cómputo de la secretaría académica por falta de mantenimiento preventivo programado por la rectoría	Establecer mecanismos de comunicación efectivos para la detección y atención oportuna de los incidentes presentados en los sistemas de información	Definir protocolos adecuados para la comunicación de incidentes, permitiendo su trazabilidad	Rector		15/01/18	30/11/18
28	Averías en el equipo de cómputo de la secretaría académica por el no reporte oportuno de las incidencias por parte de la secretaria académica	Establecer medidas que permitan garantizar el adecuado funcionamiento de los sistemas de información de la secretaría académica	Elaborar cronogramas de mantenimiento preventivo de los equipos de cómputo				
29	Demora en la atención de los usuarios por problemas de tiempo en el procesamiento de información del equipo de cómputo de la secretaría académica						
30	Demora en la atención de los usuarios por problemas relacionados con la idoneidad en el manejo del equipo de cómputo y/o software	Controlar adecuadamente la efectividad de los procesos de inducción	Establecer mecanismos que permitan verificar la efectividad de los procesos de inducción	Rector		15/01/18	30/11/18
			Establecer cronograma de reinducciones periódicas, teniendo en cuenta los resultados	Rector		15/01/18	30/11/18

N.	ESCENARIO DE RIESGO	PLAN DE MITIGACIÓN DE RIESGOS					
		ESTRATEGIA	ACTIVIDAD	RESPONSABLE	VALOR	FECHA INICIO	FECHA FINAL
	para el control académico de la IED por parte de la secretaria académica		arrojados en la evaluación de la efectividad de la inducción				
		Definir mecanismos que permitan el uso adecuado de los recursos tecnológicos del área de secretaría académica	Establecer un plan de capacitación anual para el uso adecuado de los recursos tecnológicos	Rector		15/01/18	30/11/18
		Establecer mecanismos para medir el desempeño de los funcionarios	Definir las competencias laborales y comportamentales a ser incluidas en la evaluación de desempeño relacionada con el tratamiento de la información	Rector		15/01/18	30/11/18
32	Demora en el proceso de atención de los usuarios por retraso en el proceso de ingreso de las calificaciones reportadas por los docentes al sistema de control de la IED por parte de la secretaria académica	Controlar adecuadamente la efectividad de los procesos de inducción	Establecer mecanismos que permitan verificar la efectividad de los procesos de inducción	Rector		15/01/18	30/11/18
			Establecer cronograma de reinducciones periódicas, teniendo en cuenta los resultados arrojados en la evaluación de la efectividad de la inducción	Rector		15/01/18	30/11/18
		Definir mecanismos que permitan el uso adecuado de los recursos tecnológicos del área de secretaría académica	Establecer un plan de capacitación anual para el uso adecuado de los recursos tecnológicos	Rector		15/01/18	30/11/18
		Establecer mecanismos para medir el desempeño de los funcionarios	Definir las competencias laborales y comportamentales a ser incluidas en la evaluación de desempeño relacionada con el tratamiento de la información	Rector		15/01/18	30/11/18

N.	ESCENARIO DE RIESGO	PLAN DE MITIGACIÓN DE RIESGOS					
		ESTRATEGIA	ACTIVIDAD	RESPONSABLE	VALOR	FECHA INICIO	FECHA FINAL
33	Desatención del equipo de procesamiento de datos y archivo por citaciones a reuniones constantes en horarios habilitados para atención al público por parte del rector	Revisar las políticas rectorales para los horarios establecidos para reuniones generales	Ajustar las políticas de horarios de reunión en procura que no exista afluencia de público cuando estas se lleven a cabo	Rector		15/01/18	30/11/18
		Establecer directrices para garantizar que la información de los estudiantes y docentes no es evidente a simple vista por personal no autorizado en las zonas de atención al público	Definir protocolos de seguridad cuando el equipo de cómputo se encuentra desatendido	Rector		15/01/18	30/11/18
			Definir protocolos de prevención de exposición de la información en el escritorio de la secretaría académica	Rector		15/01/18	30/11/18
35	Fallos o demoras en la atención del público por afectación de software malicioso en el equipo de cómputo de la secretaría académica	Establecer mecanismos de comunicación efectivos para la detección y atención oportuna de los incidentes presentados en los sistemas de información	Definir protocolos adecuados para la comunicación de incidentes, permitiendo su trazabilidad	Rector		15/01/18	30/11/18
		Establecer políticas para el manejo adecuado de dispositivos móviles y unidades de almacenamiento extraíble en el área de archivo de la secretaría académica	Revisar y complementar las disposiciones rectorales sobre el manejo de dispositivos móviles y unidades de almacenamiento extraíbles en el área de archivo	Rector		15/01/18	30/11/18
		Establecer medidas que permitan garantizar el adecuado funcionamiento de los sistemas de información de la secretaría académica	Elaborar cronogramas de mantenimiento preventivo de los equipos de cómputo	Rector		15/01/18	30/11/18
36	Afectación del equipo de la secretaría académica por software malicioso a causa del uso inadecuado del recurso por parte del	Establecer mecanismos de comunicación efectivos para la detección y atención oportuna de los incidentes presentados en los sistemas de información	Definir protocolos adecuados para la comunicación de incidentes, permitiendo su trazabilidad	Rector		15/01/18	30/11/18

N.	ESCENARIO DE RIESGO	PLAN DE MITIGACIÓN DE RIESGOS					
		ESTRATEGIA	ACTIVIDAD	RESPONSABLE	VALOR	FECHA INICIO	FECHA FINAL
	personal de la secretaría académica	Establecer políticas para el manejo adecuado de dispositivos móviles y unidades de almacenamiento extraíble en el área de archivo de la secretaría académica	Revisar y complementar las disposiciones rectorales sobre el manejo de dispositivos móviles y unidades de almacenamiento extraíbles en el área de archivo				
		Establecer medidas que permitan garantizar el adecuado funcionamiento de los sistemas de información de la secretaría académica	Elaborar cronogramas de mantenimiento preventivo de los equipos de cómputo				
37	Afectaciones de las comunicaciones por infección de software malicioso que incide en los drivers de la tarjeta de red del computador de la secretaría académica	Definir mecanismos que permitan el uso adecuado de los recursos tecnológicos del área de secretaría académica	Establecer un plan de capacitación anual para el uso adecuado de los recursos tecnológicos				
38	Pérdida del archivo físico de los estudiantes y docentes por ocurrencia de desastre natural (terremoto, derrumbe, inundación, etc.)	Elaboración de mecanismos de prevención y respuesta a desastres naturales	Establecimiento de plan de contingencia para atención de incidentes provocados por fuego	Rector		15/01/18	30/11/18
			Establecimiento de plan de contingencia para atención de incidentes provocados por inundación				
			Establecimiento de plan de contingencia para atención de incidentes provocados por terremoto				

N.	ESCENARIO DE RIESGO	PLAN DE MITIGACIÓN DE RIESGOS					
		ESTRATEGIA	ACTIVIDAD	RESPONSABLE	VALOR	FECHA INICIO	FECHA FINAL
		Establecer mecanismos de reacción en caso de incidentes ocasionados por fuego	Definir un plan de capacitación en el manejo de extintores en convenio con la ARL				
		Establecer procedimientos de copia de seguridad	Definir protocolos para generar copias de seguridad				
39	Pérdida del equipo de cómputo e información digital de la secretaría académica por ocurrencia de desastre natural (terremoto, derrumbe, inundación, etc.)	Establecer un procedimiento documentado para garantizar la continuidad de las actividades del área de secretaría académica	Definir un procedimiento que defina las directrices para garantizar la continuad de la prestación del servicio	Rector		15/01/18	30/11/18
40	Pérdida de las comunicaciones para el reporte a la Secretaría de Educación y/o entidades externas por daños en los sistemas de comunicación ocasionados por desastres naturales	Elaboración de mecanismos de respuesta a fallos en las comunicaciones	Establecimiento de plan de contingencia con los proveedores de servicios	Rector		15/01/18	30/11/18
		Establecer mecanismos de comunicación efectivos para la detección y atención oportuna de los incidentes presentados en los sistemas de información	Definir protocolos adecuados para la comunicación de incidentes, permitiendo su trazabilidad				
		Establecer mecanismos de reacción en caso de incidentes ocasionados por fuego	Definir un plan de capacitación en el manejo de extintores en convenio con la ARL	Rector		15/01/18	30/11/18
41	Pérdida de información en el equipo de cómputo de la secretaría académica por fallos del fluido eléctrico	Establecer procedimientos de copia de seguridad	Definir protocolos para generar copias de seguridad	Rector		15/01/18	30/11/18
42	Daño en el software de control académico por	Establecer mecanismos que protejan los dispositivos de sobre voltajes y/o fallos en la prestación del servicio de energía	Incluir en el plan de adquisiciones UPS, planta eléctrica, plan de mantenimiento del tendido eléctrico				

N.	ESCENARIO DE RIESGO	PLAN DE MITIGACIÓN DE RIESGOS					
		ESTRATEGIA	ACTIVIDAD	RESPONSABLE	VALOR	FECHA INICIO	FECHA FINAL
	fallos en el fluido eléctrico						
43	Parálisis del proceso de matrícula por fallos en el fluido eléctrico	Establecer un procedimiento documentado para garantizar la continuidad de las actividades del área de secretaría académica	Definir un procedimiento que defina las directrices para garantizar la continuidad de la prestación del servicio				
44	Retrasos en el proceso de ingreso de calificaciones por fallos en el fluido eléctrico						
46	Afectación física en el personal del área de secretaría académica por fuego provocado y ausencia de planes de emergencia y/o rutas adecuadas de evacuación	Elaboración de mecanismos de prevención y respuesta a desastres naturales	Establecimiento de plan de contingencia para atención de incidentes provocados por fuego	Rector		15/01/18	30/11/18
		Establecer mecanismos de reacción en caso de incidentes ocasionados por fuego	Definir un plan de capacitación en el manejo de extintores en convenio con la ARL	Rector		15/01/18	30/11/18
		Establecer un procedimiento documentado para garantizar la continuidad de las actividades del área de secretaría académica	Definir un procedimiento que defina las directrices para garantizar la continuidad de la prestación del servicio	Rector		15/01/18	30/11/18
47	Deterioro del archivo físico de los estudiantes y los docentes por corrosión provocada por humedad	Establecer mecanismos que protejan la información física y los dispositivos almacenados en el archivo de corrosión provocada por la humedad	Incluir en el plan de adquisiciones plan de mantenimiento de la infraestructura del área de secretaría académica	Rector		15/01/18	30/11/18
49	Interceptación de datos de los estudiantes por infección con software espía por deficiencias en los mecanismos de protección tales como antivirus y antimalware	Establecer mecanismos de comunicación efectivos para la detección y atención oportuna de los incidentes presentados en los sistemas de información	Definir protocolos adecuados para la comunicación de incidentes, permitiendo su trazabilidad	Rector		15/01/18	30/11/18
		Establecer procedimientos de copia de seguridad	Definir protocolos para generar copias de seguridad	Rector		15/01/18	30/11/18

N.	ESCENARIO DE RIESGO	PLAN DE MITIGACIÓN DE RIESGOS					
		ESTRATEGIA	ACTIVIDAD	RESPONSABLE	VALOR	FECHA INICIO	FECHA FINAL
		Establecer medidas que permitan garantizar el adecuado funcionamiento de los sistemas de información de la secretaría académica	Elaborar cronogramas de mantenimiento preventivo de los equipos de cómputo	Rector		15/01/18	30/11/18
		Establecer las directrices y parámetros para la contratación de proveedores	Definir los requisitos en términos de seguridad de la información que los proveedores de servicios de tecnología deben tener en cuenta al prestar servicios a la IED	Rector		15/01/18	30/11/18
50	Divulgación de la información de los estudiantes y/o docentes por medio de la práctica inadecuada de desecho de información reciclada por parte de la secretaria académica	Concientizar al personal de la secretaría académica sobre la importancia de preservar adecuadamente la información de los niños, niñas, adolescentes y docentes	Establecer un cronograma de capacitaciones sobre la Ley 1581/2012 y las disposiciones del MEN en términos de protección de la información de los estudiantes y docentes	Rector		15/01/18	30/11/18
		Establecer mecanismos que garanticen que la información desechada en medios físicos o digitales es tratada adecuadamente	Definir políticas para el tratamiento de los desechos que pueden poner en riesgo la información confidencial de los niños, niñas, adolescentes y docentes				
51	Divulgación de la información de los estudiantes y/o docentes por falta de políticas y mecanismos para la adecuada disposición de los desechos	Establecer mecanismos que garanticen la adecuada disposición de los residuos físicos	Incluir en el plan de adquisiciones la compra de una máquina pica papel				
52	Fallos en el funcionamiento del equipo de cómputo de la	Establecer mecanismos de comunicación efectivos para la detección y atención oportuna	Definir protocolos adecuados para la comunicación de	Rector		15/01/18	30/11/18

N.	ESCENARIO DE RIESGO	PLAN DE MITIGACIÓN DE RIESGOS					
		ESTRATEGIA	ACTIVIDAD	RESPONSABLE	VALOR	FECHA INICIO	FECHA FINAL
	secretaría académica por instalación de software pirata, ocasionado por falta de políticas con los proveedores, y el personal de la IED	de los incidentes presentados en los sistemas de información	incidentes, permitiendo su trazabilidad				
		Establecer procedimientos de copia de seguridad	Definir protocolos para generar copias de seguridad				
		Establecer medidas que permitan garantizar el adecuado funcionamiento de los sistemas de información de la secretaría académica	Elaborar cronogramas de mantenimiento preventivo de los equipos de cómputo				
		Establecer las directrices y parámetros para la contratación de proveedores	Definir los requisitos en términos de seguridad de la información que los proveedores de servicios de tecnología deben tener en cuenta al prestar servicios a la IED				
53	Divulgación y daño en la información confidencial de los estudiantes y/o docentes por retaliaciones políticas en periodos de elecciones por falta de políticas de confidencialidad	Establecer mecanismos que permitan preservar la información confidencial	Definir acuerdos de confidencialidad con los funcionarios del área de secretaría académica	Rector		15/01/18	30/11/18
54	Exposición de las contraseñas de acceso a los equipos de cómputo y sistemas de información por falta de medidas de prevención, uso adecuado y preservación de las mismas	Establecer directrices para garantizar que la información relacionada con las claves de acceso a los sistemas de información no es evidente a simple vista por personal no autorizado en las zonas de atención al público	Definir protocolos de seguridad cuando el equipo de cómputo se encuentra desatendido	Rector		15/01/18	30/11/18
			Definir protocolos de prevención de exposición de la información en el escritorio de la secretaría académica				

N.	ESCENARIO DE RIESGO	PLAN DE MITIGACIÓN DE RIESGOS					
		ESTRATEGIA	ACTIVIDAD	RESPONSABLE	VALOR	FECHA INICIO	FECHA FINAL
		Establecer procedimientos documentados para el adecuado manejo de las claves de acceso al equipo de cómputo y a los Sistemas de Información	Definir protocolos de manejo adecuado de claves				
55	Demora en el restablecimiento del servicio por fallos relacionados a la extracción de copias de seguridad y pruebas de las mismas	Establecer los protocolos para generar y probar las copas de seguridad del área de secretaría académica	Definir el protocolo para la extracción y prueba de las copias de seguridad, almacenamiento y cronograma de ejecución	Rector		15/01/18	30/11/18
		Establecer los medios de almacenamiento de las copias de seguridad	Incluir en el plan de adquisiciones los dispositivos necesarios para el almacenamiento de las copias de seguridad				

4.1.3.15. Paso 15: Declaración de aplicabilidad

R = Riesgos, Observaciones = Obs; Obligatorio =

A.5	**Políticas de la Seguridad de la Información**				
A.5.1	**Orientación de la dirección para la gestión de la seguridad de la información**				
Objetivo de Control: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes					
COD.	**CONTROL**	**DESCRIPCIÓN DEL CONTROL**	**EXISTENTE**	**PROPUESTO**	**OBS**
A.5.1.1	Política para la seguridad de la información	Se debe definir un conjunto de políticas para la seguridad de la información aprobadas por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes	1, 3, 4, 5, 7, 8, 14, 15, 16, 17, 18, 19, 20, 22, 23, 33, 54	50, 51	

COD.	CONTROL	DESCRIPCIÓN DEL CONTROL	EXISTENTE	PROPUESTO	OBS
A.5.1.2	Revisión de las políticas para la seguridad de la Información	Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúa.		7, 8, 23, 35, 36, 37	
A.6	**Organización de la seguridad de la información**				
A.6.2	**Dispositivos Móviles y Teletrabajo**				
Objetivo de Control: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles					
COD.	**CONTROL**	**DESCRIPCIÓN DEL CONTROL**	**EXISTENTE**	**PROPUESTO**	**OBS**
A.6.2.1	Política para dispositivos móviles	Se deben adoptar una política y unas medidas de seguridad de soporte para gestionar los riesgos introducidos por el uso de dispositivos móviles.	7, 8, 9, 23, 35, 36, 37		
A.7	**Seguridad de los recursos humanos**				
A.7.1	**Antes de asumir el empleo**				
Objetivo de Control: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran					
COD.	**CONTROL**	**DESCRIPCIÓN DEL CONTROL**	**EXISTENTE**	**PROPUESTO**	**OBS**
A.7.1.2	Término y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	2, 24, 30, 31		Sólo aplica para contratistas
A.7.2	**Durante la ejecución del empleo**				
Objetivo de Control: Asegurarse que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.					
COD.	**CONTROL**	**DESCRIPCIÓN DEL CONTROL**	**EXISTENTE**	**PROPUESTO**	**OBS**
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Todos los empleados de la organización y en donde sea pertinente los contratistas deben recibir la educación y la formación en toma de conciencia apropiada y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	2, 6, 11, 24, 26, 30, 31, 32	1, 5, 14, 15, 36, 37, 50	
A.7.3	**Terminación y cambio de empleo**				
Objetivo de Control: Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.					
COD.	**CONTROL**	**DESCRIPCIÓN DEL CONTROL**	**EXISTENTE**	**PROPUESTO**	**OBS**
A.7.3.1	Terminación y cambio de responsabilidades de empleo.	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se debe definir, comunicar al empleado o contratista y se debe hacer cumplir.		23, 24	

A.8	**Gestión de activos**
A.8.1	**Responsabilidad por los activos**

Objetivo de Control: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.

COD.	CONTROL	DESCRIPCIÓN DEL CONTROL	EXISTENTE	PROPUESTO	OBS
A.8.1.1	Inventario de activos	Se deben identificar los activos asociados con la información e instalaciones de procesamiento de información y se debe elaborar y mantener un inventario de estos activos.		3, 4, 7, 16, 22, 23	
A.8.1.2	Propiedad de los activos	Los activos mantenidos en el inventario deben tener un propietario.		3, 4, 7, 16, 22, 23	
A.8.1.3	Uso aceptable de los activos.	Se deben identificar documentar e implementar reglas para el uso aceptable de la información y de activos asociados con información e instalaciones de procesamiento de información.		26, 30, 32, 36, 37	

A.8.2	**Clasificación de la información**

Objetivo de Control: Asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.

COD.	CONTROL	DESCRIPCIÓN DEL CONTROL	EXISTENTE	PROPUESTO	OBS
A.8.2.1	Clasificación de la información	La información se debe clasificar en función de los requisitos legales valor criticidad y susceptibilidad a divulgación o a modificación no autorizada.		3, 4, 7, 16, 22, 23	
A.8.2.3	Manejo de activos	Se deben desarrollar e implementar un conjunto adecuado de procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.		1, 3, 4, 7, 16, 17, 18, 19, 20, 22, 23, 26, 30, 32, 33, 36, 37, 50, 54	

A.8.3	**Manejo de activos**

Objetivo de Control: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios

COD.	CONTROL	DESCRIPCIÓN DEL CONTROL	EXISTENTE	PROPUESTO	OBS
A.8.3.1	Gestión de medios removibles	Se deben implementar procedimientos para gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	7, 8, 9, 35, 36, 37		
A.8.3.2	Disposición de los medios	Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.		8, 35, 36, 37, 50, 51	
A.8.3.3	Transferencia de medios físicos	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el trasporte.		8, 35, 36, 37	

A.9	Control de acceso				
A.9.1	**Requisitos del negocio para control de acceso**				
Objetivo de Control: Limitar el acceso a información y a instalaciones de procesamiento de información					
COD.	**CONTROL**	**DESCRIPCIÓN DEL CONTROL**	**EXISTENTE**	**PROPUESTO**	**OBS**
A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	3, 4, 5, 7, 16, 22, 23, 54		
A.9.2	**Gestión de acceso a usuarios**				
Objetivo de Control: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios					
COD.	**CONTROL**	**DESCRIPCIÓN DEL CONTROL**	**EXISTENTE**	**PROPUESTO**	**OBS**
A.9.2.1	Registro y cancelación del registro de usuarios	Implementar un proceso formal de registro y de cancelación de registro de usuarios para posibilitar la asignación de los derechos de acceso.		1, 5, 8, 17, 18, 19, 20, 22, 23, 54	
A.9.2.2	Suministro de acceso de usuarios	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.		1, 5, 8, 17, 18, 19, 20, 22, 23, 54	
A.9.2.3	Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.		1, 5, 8, 17, 18, 19, 20, 22, 23, 54	
A.9.2.4	Gestión de Información de autenticación secreta de usuarios	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal		1, 5, 8, 17, 18, 19, 20, 22, 23, 54	
A.9.2.5	Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.		1, 5, 8, 17, 18, 19, 20, 22, 23, 54	
A.9.2.6	Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.		1, 5, 8, 17, 18, 19, 20, 22, 23, 54	
A.9.3	**Responsabilidades de los usuarios**				
Objetivo de Control: Hacer que los usuarios rindan cuenta por la salvaguarda de su información de autenticación					
COD.	**CONTROL**	**DESCRIPCIÓN DEL CONTROL**	**EXISTENTE**	**PROPUESTO**	**OBS**
A.9.3.1	Uso de la información de autenticación secreta	Se debe exigir a los usuarios que cumplan las prácticas de la organización para uso de información de autenticación secreta.		1, 5, 8, 17, 18, 19, 20, 22, 23, 54	

A.9.4	**Control de acceso a sistemas o aplicaciones**				
Objetivo de Control: Evitar el acceso no autorizado a sistemas y aplicaciones					
COD.	**CONTROL**	**DESCRIPCIÓN DEL CONTROL**	**EXISTENTE**	**PROPUESTO**	**OBS**
A.9.4.1	Restricción de acceso de información	El acceso a la formación y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.		1, 5, 8, 17, 18, 19, 20, 22, 23, 54	
A.9.4.2	Procedimiento de ingreso seguro	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.		1, 5, 8, 17, 18, 19, 20, 22, 23, 54	
A.9.4.3	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	1, 5, 17, 18, 19, 20, 21, 22, 23, 34	8, 54	
A11	**Seguridad física y del entorno**				
A.11.1	**Áreas seguras**				
Objetivo de Control: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y las instalaciones de procesamientos de información de la organización					
COD.	**CONTROL**	**DESCRIPCIÓN DEL CONTROL**	**EXISTENTE**	**PROPUESTO**	**OBS**
A.11.1.1	Perímetro de seguridad física	Se deben definir y usar perímetros de seguridad y usarlos para proteger las áreas que contenga información confidencial o critica, e instalaciones de manejo de información.	1, 3, 4, 8, 16, 17, 18, 22, 23, 25		
A.11.1.2	Controles de acceso físicos	Las áreas seguras que se deben proteger mediante controles de acceso apropiados para asegurar que solo se permita el acceso a personal autorizado.	1, 3, 4, 8, 10, 13, 16, 17, 18, 19, 20, 21, 22, 23, 25, 34		
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	3, 4, 10, 13, 16, 17, 18, 19, 20, 21, 22, 23, 25		
A.11.1.4	Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	3, 4, 10, 13, 16, 17, 18, 19, 20, 21, 22, 23, 25, 38, 39, 45, 46, 47		
A.11.1.6	Áreas de despacho y cargas	Se deben controlar los puntos de acceso tales como áreas de despachos y de carga y otros puntos en donde puedan entrar personas no autorizadas y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	3, 4, 10, 13, 16, 17, 18, 19, 20, 21, 22, 23, 25		

A.11.2	**Equipos**

Objetivo de Control: Prevenir la pérdida, daño, robo o compromiso de activos y la interrupción de las operaciones de la organización

COD.	CONTROL	DESCRIPCIÓN DEL CONTROL	EXISTENTE	PROPUESTO	OBS
A.11.2.1	Ubicación y protección de equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno y las posibilidades de acceso no autorizado.		1, 17, 18, 19, 20, 22, 23, 33, 54	
A.11.2.2	Servicios de suministro	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.		41, 42, 41, 44, 55	
A.11.2.3	Seguridad del cableado	El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.		10, 41, 42, 43, 44	
A.11.2.4	Mantenimiento de equipos	Los equipos se deben mantener correctamente para asegurar disponibilidad e integridad continuas.		12, 27, 28, 29, 35, 36, 37, 49, 52	
A.11.2.8	Equipos de usuario desatendido	Los usuarios deben asegurar que a los equipos desatendidos se les da protección apropiada.		1, 17, 18, 19, 20, 22, 23, 33, 54	
A.11.2.9	Política de escritorio limpio y pantalla limpia	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles y una política de pantalla limpia en las instalaciones de procesamiento de información.		1, 17, 18, 19, 20, 22, 23, 33, 54	

A12	**Seguridad de las operaciones**
A.12.1	**Procedimientos operacionales y responsabilidades**

Objetivo de Control: Asegurar las operaciones correctas y asegurarse de las instalaciones de procesamiento de información

COD.	CONTROL	DESCRIPCIÓN DEL CONTROL	EXISTENTE	PROPUESTO	OBS
A.12.1.1	Procedimientos de operación documentados	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	2, 6, 11, 24, 26, 30, 31, 32		
A.12.1.2	Gestión de cambios	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	2, 6, 11, 24, 26, 30, 31, 32		

A.12.2	**Protección contra códigos maliciosos**

Objetivo de Control: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.

COD.	CONTROL	DESCRIPCIÓN DEL CONTROL	EXISTENTE	PROPUESTO	OBS
A.12.2.1	Controles contra códigos maliciosos	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	35, 36, 37, 48, 49		

A.12.3	**Copias de respaldo**

Objetivo de Control: Proteger contra la pérdida de datos

COD.	CONTROL	DESCRIPCIÓN DEL CONTROL	EXISTENTE	PROPUESTO	OBS
A.12.3.1	Respaldo de la información	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.		1, 5, 38, 39, 41, 42, 43, 44, 49, 52, 55	

A13	**Seguridad de las comunicaciones**
A.13.2	**Transferencia de información**

Objetivo de Control: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa

COD.	CONTROL	DESCRIPCIÓN DEL CONTROL	EXISTENTE	PROPUESTO	OBS
A.13.2.2	Acuerdos sobre transferencia de información	Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.		15	
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información.		14, 49, 52, 53	

A.15	**Relaciones con los proveedores**
A.15.1	**Seguridad de la información en las relaciones con los proveedores**

Objetivo de Control: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores

COD.	CONTROL	DESCRIPCIÓN DEL CONTROL	EXISTENTE	PROPUESTO	OBS
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.		12, 49, 52	
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con los proveedores	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	27, 28, 29, 35, 36, 40, 41, 42, 47, 48, 49, 52, 55		
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	27, 28, 29, 35, 36, 40, 41, 42, 47, 48, 49, 52, 55		

A.15.2	**Gestión de la prestación de servicios de proveedores**

Objetivo de Control: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores

COD.	CONTROL	DESCRIPCIÓN DEL CONTROL	EXISTENTE	PROPUESTO	OBS
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.		12, 40, 49, 52	
A.15.2.2	Gestión de cambios en los servicios de los proveedores	Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimiento y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos.		12, 40, 49, 52	

A16	**Gestión de incidentes de seguridad de la información**
A.16.1	**Gestión de incidentes y mejoras en la seguridad de la información**

Objetivo de Control: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades

COD.	CONTROL	DESCRIPCIÓN DEL CONTROL	EXISTENTE	PROPUESTO	OBS
A.16.1.1	Responsabilidades y procedimientos	Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.		12, 16, 26, 27, 28, 29, 35, 36, 37, 40, 49, 52	
A.16.1.2	Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	6, 11, 12, 26, 27, 28, 29, 35, 36, 37, 40, 49, 52		
A.16.1.3	Reporte de debilidades de seguridad de la información	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	6, 11, 12, 26, 27, 28, 29, 35, 36, 37, 40, 49, 52		
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.		12, 26, 27, 28, 29, 35, 36, 37, 40, 49, 52	
A.16.1.5	Respuesta a incidentes de seguridad de la información	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	12, 26, 27, 28, 29, 35, 36, 37, 40, 41, 42, 47, 48, 49, 52, 55		
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.		12, 26, 27, 28, 29, 35, 36, 37, 40, 49, 52	

COD.	CONTROL	DESCRIPCIÓN DEL CONTROL	EXISTENTE	PROPUESTO	OBS
A.16.1.7	Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.		12, 26, 27, 28, 29, 35, 36, 37, 40, 49, 52	
A18	**Cumplimiento**				
A.18.1	**Cumplimiento de requisitos legales y contractuales**				
Objetivo de Control: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad					
COD.	**CONTROL**	**DESCRIPCIÓN DEL CONTROL**	**EXISTENTE**	**PROPUESTO**	**OBS**
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización.		1, 5, 14, 50, 51	
A.18.1.3	Protección de registros	Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos de reglamentación, contractuales y de negocio.		1, 5, 14, 50, 51	
A.18.1.4	Privacidad y protección de información de datos personales	Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.		1, 5, 14, 50, 51	MEN y Ley 1581/12
A.18.2	**Revisiones de seguridad de la información**				
Objetivo de Control: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales					
COD.	**CONTROL**	**DESCRIPCIÓN DEL CONTROL**	**EXISTENTE**	**PROPUESTO**	**OBS**
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidades, con las políticas y normas de seguridad apropiadas, y cualquier otro y cualquier otro requisito de seguridad.		2, 15, 24, 30, 32	

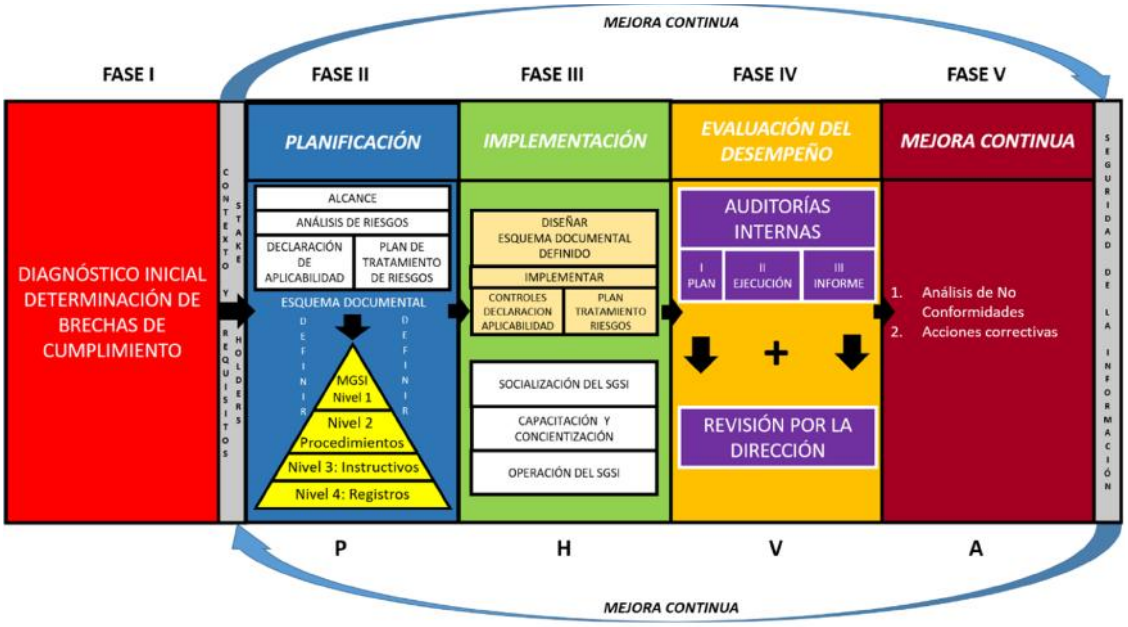
5. Concreción del modelo

El modelo propuesto fue diseñado siguiendo las mejores prácticas propuestas por MINTIC, para el logro de los objetivos de la Estrategia de Gobierno en Línea y las disposiciones legales del MEN, de igual manera ha sido determinado por los resultados obtenidos en los diagnósticos iniciales, así como el análisis del contexto de las IED's de la Comuna Universidad de la Ciudad de Pereira, identificando sus necesidades, requisitos de seguridad, controles de seguridad existentes y documentación tipo necesaria para la implementación del SGSI.

El Modelo de Gestión de Seguridad de la Información conduce a garantizar la confidencialidad, integridad y disponibilidad de la información de las IED's, empleando para tal fin una metodología definida para la gestión del riesgo.

5.1.Esquema general del modelo

Las fases propuestas se encuentran alineadas con el Modelo de seguridad y privacidad establecido por MINTIC, esquematizando la relación secuencial y las actividades relevantes en cada una de ellas, tal como se aprecia en la gráfica 55, facilitando el diseño e implementación por los directivos de las IED's y sus equipos de trabajo.



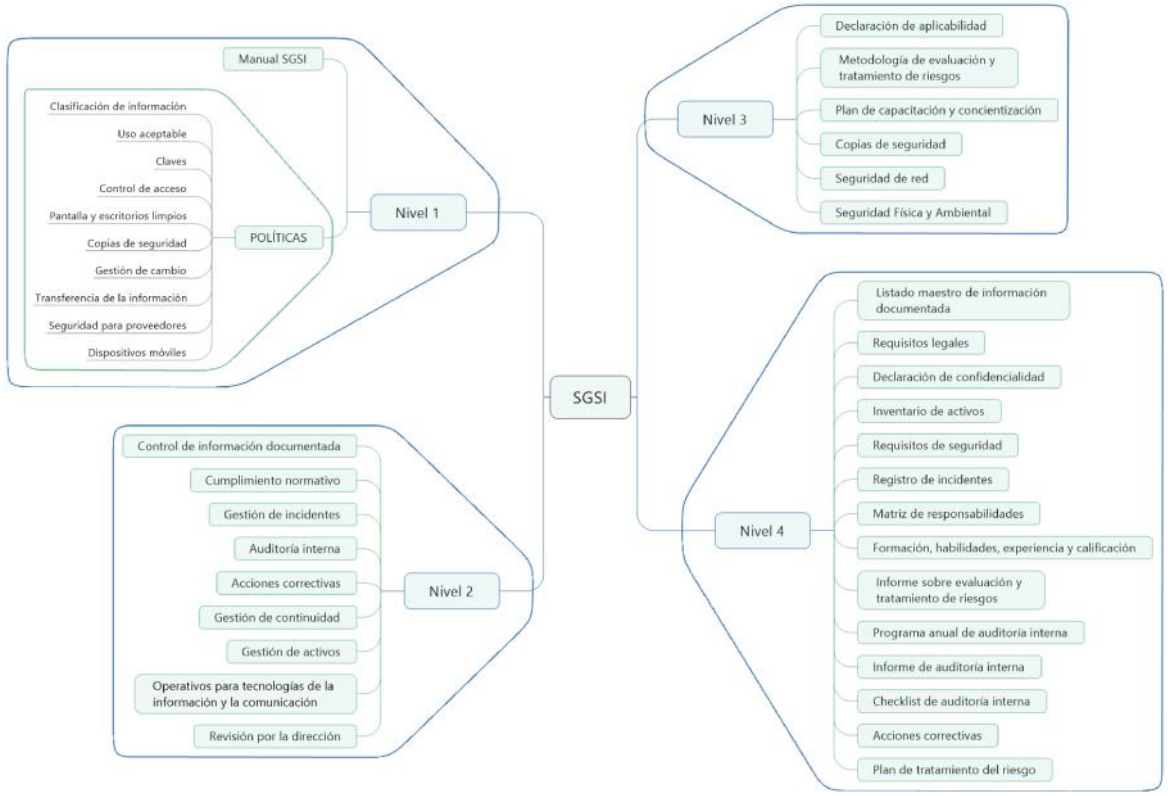
Gráfica 55. Esquema general del modelo de SGSI propuesto.

Fuente: Propia

Se establece de igual manera una correspondencia entre los requisitos exigidos por la Norma Internacional NTC ISO/IEC 27001:2013 y las actividades planteadas.

5.2.Esquema documental base

La documentación base está conformada por 4 niveles, organizados de forma piramidal, los cuales se ilustran en la gráfica 56; es importante resaltar que se propone la documentación de manera general, pero es la IED quien en la fase de planeación deberá definir la documentación que de acuerdo a sus necesidades particulares identifique.



Gráfica 56. Esquema documental base.

Fuente: Propia

Nivel 1: Contiene el Manual del Sistema de Gestión de Seguridad de la Información, el alcance, objetivos, responsabilidades y políticas adoptadas por la IED.

Nivel 2: En esta categoría se encuentran los procedimientos que permiten garantizar el cumplimiento de los procesos de seguridad de la información.

Nivel 3: Abarca instructivos que relacionan las actividades específicas relacionadas a las actividades de la seguridad de la información y complementarios a los documentos del nivel 2.

Nivel 4: Constituyen la evidencia de la ejecución de las actividades y por ende la base de verificación para las auditorías.

5.2.1. Fase I – Diagnóstico inicial

El objetivo de esta fase es determinar el grado de cumplimiento de la IED con relación a la totalidad de requisitos establecidos en la Norma Internacional NTC ISO/IEC 27001:2013, para llevar a cabo esta actividad se recomienda la implementación del instrumento descrito en el apartado 4.1.1 del presente documento.

5.2.2. Fase II - Planificación

En esta fase la IED llevará acabo el análisis de riesgos, para lo cual se recomienda seguir los pasos descritos en el numeral 4.1.3 de este documento y que se compone de las siguientes etapas:

1. Definición del alcance: se debe identificar de manera clara y precisa el alcance del SGSI, para de esta manera tenerlo presente al iniciar la etapa de análisis de riesgos.
2. Análisis de riesgos: se lleva a cabo el proceso descrito detalladamente en el numeral 4.1.3 del presente documento y que comprende las siguientes actividades:
    a. Definir del alcance
    b. Generar inventario de activos
    c. Identificar los factores de criticidad de activos.

d. Identificar los niveles de criticidad de los activos

e. Identificar los escenarios de riesgos

f. Determinar la calificación de la probabilidad

g. Determinar la calificación del impacto potencial

h. Calcular la vulnerabilidad inherente

i. Definir los criterios de aceptabilidad del riesgo

j. Elaborar los mapas de temperatura de vulnerabilidad inherente

k. Identificar los controles de mitigación de riesgos existentes

l.

m. Generar un plan de tratamiento de riesgos

n. Calcular la vulnerabilidad residual

o. Elaborar los mapas de temperatura de vulnerabilidad residual

3. Definir la documentación necesaria: se identifica la documentación necesaria en virtud de los resultados obtenidos en el análisis de riesgos. El desarrollo de esta fase se realiza por niveles documentales, tal como se describe en el "Esquema documental base", a continuación, se explican los documentos correspondientes a cada uno de ellos.

Nivel 1

Manual del SGSI: constituye la columna vertebral del SGSI, contiene las disposiciones generales adoptadas por la IED, debe contener mínimo los siguientes tópicos, sin ser este un orden estricto y obligatorio, los procedimientos mencionados

en el manual no se desarrollan en éste solo se presentan debido a que pertenecen al Nivel 2 de la documentación:

1. Objetivo
2. Alcance: define claramente los límites del SGSI en la IED, sus usuarios y a quiénes es aplicable.
3. Política de seguridad de la información: establece las reglas básicas para la gestión de la seguridad de la información, al igual el alcance de su aplicación y los usuarios de la misma.
4. Compromiso de la dirección: declaración expresa del compromiso y apoyo de la rectoría con la protección de la información institucional.
5. Objetivos y metas de seguridad de la información.
6. Responsabilidades: define cuales son los organismos internos o cargos responsables de que el manual del SGSI se mantenga controlado.
7. Metodología de evaluación y tratamiento de riesgos: se presenta de manera general, la estrategia metodológica que aborda la IED para realizar la gestión de riesgos, su descripción detallada pertenece al Nivel 3 de la documentación.
8. Procedimientos: estos documentos son de Nivel 2, y se detallan en la gráfica 56.
9. Políticas complementarias del SGSI
    a. Clasificación de información: garantiza la protección de la información a niveles adecuados de acuerdo con la sensibilidad de la misma, asignación de recursos necesarios para la aplicación de controles y la

preservación de la confidencialidad, integridad y disponibilidad de la misma.

b. Uso aceptable: define las condiciones de uso de los sistemas y demás activos relacionados a la gestión de la información.

c. Claves: define el conjunto de reglas que establecen el modo de generación, almacenamiento, distribución, borrado, actualización, recuperación, protección y aplicación de claves en los sistemas de información de la IED. Así mismo define quienes son los responsables de estas actividades.

d. Control de acceso: define las condiciones de acceso a los sistemas, equipos, instalaciones e información de conformidad con los requerimientos establecidos por el MEN, la IED y la seguridad.

e. Pantalla y escritorios limpios: define las pautas que permiten reducir el riesgo de acceso no autorizado, pérdida y daño de la información dentro y fuera del horario normal de trabajo de los usuarios.

f. Copias de seguridad: define los medios de respaldo adecuados para asegurar que todo software e información esencial se pueda recuperar después de una falla, así mismo los intervalos de respaldo y verificación de las copias almacenadas.

g. Gestión de cambio: define los controles necesarios para realizar cambios en los sistemas de información.

h. Transferencia de la información: define los mecanismos que aseguran la seguridad de la información y el software cuando son intercambiados dentro y fuera de la IED.

i. Seguridad para proveedores: define las reglas básicas para la relación con los proveedores.

j. Dispositivos móviles: define los términos de uso de los dispositivos ubicados tanto al interior como al exterior de la IED, así mismo su aplicabilidad y usuarios.

10. Declaración de aplicabilidad: en este apartado se describe de manera general la declaración de aplicabilidad, se indica el alcance y los usuarios de la misma, el documento de la declaración de aplicabilidad se incluye en el Nivel 3 de la documentación, y se define como documento base la declaración detallada en el numeral 4.1.3.11 del presente documento.

Nivel 2

Se compone de los siguientes documentos:

1. Control de información documentada: asegura el control sobre la creación, aprobación, uso y actualización de la información documentada empleada en el SGSI, define el alcance de su aplicación, las formas de almacenamiento de la información documentada y los usuarios del documento.
2. Cumplimiento normativo: define el proceso de identificación de las partes interesadas, requisitos legales, contractuales, y de otra índole relacionados con la seguridad de la información y la continuidad de la IED.

3. Gestión de incidentes: garantiza la detección temprana de eventos y debilidades de seguridad, al igual que la oportuna reacción y respuesta a incidentes de seguridad, es aplicable a todo el alcance del SGSI y sus usuarios son todos los colaboradores de la IED, proveedores y personas externas que entran en contacto con los sistemas de información.
4. Auditoría interna: describe las actividades relacionadas con la ejecución de auditorías, incluyendo el plan, selección de auditores e informes. Así mismo especifica la aplicación a todas las actividades realizadas dentro del SGSI de la IED, y los usuarios del documento.
5. Acciones correctivas: describe la metodología que se empleará para la eliminación de la causa de las No Conformidades asociadas con los requisitos del SGSI, con el fin de prevenir que ocurran nuevamente. Así mismo establece quiénes son los usuarios del documento y el alcance del mismo.
6. Gestión de continuidad: define la manera en la cual se debe desarrollar el plan de continuidad que identifica como la IED recupera su infraestructura y servicios de TI dentro de los tiempos establecidos en caso de que se materialice un desastre o incidente que detenga la operación normal, describe el alcance y los usuarios del mismo.
7. Gestión de activos: define los procedimientos para identificar y elaborar el inventario de activos de información, así mismo específica el responsable de consolidar y administrar dichos activos.

8. Operativos para tecnologías de la información y la comunicación: garantiza el funcionamiento y seguridad de la información y comunicación, su estructura básica debería estar compuesta de los siguientes ítems:
    a. Gestión de cambio (Nivel 1)
    b. Copias de seguridad (Nivel 1)
        i. Creación de copias de seguridad (Nivel 3)
        ii. Prueba de copias de seguridad (Nivel 3)
    c. Seguridad de red (Nivel 3)
    d. Servicios de red (Nivel 3)
    e. Transferencia de la información (Nivel 1)
        i. Canales de comunicación electrónica (Nivel 3)
    f. Supervisión del sistema (Nivel 3)
9. Revisión por la dirección: establece los lineamientos y periodicidad para llevar a cabo las revisiones por la rectoría al SGSI.

Nivel 3

Se compone de los siguientes instructivos

1. Declaración de aplicabilidad: se toma como base la declaración expresada en el numeral 4.1.3.11, de conformidad con los riesgos identificados en la etapa de análisis de riesgos.
2. Metodología de evaluación y tratamiento de riesgos: describe la metodología de riesgos que la IED va a emplear para realizar la gestión de riesgos, se propone

como metodología la expuesta en el numeral 4.1.3, sin ser esta de obligatorio seguimiento, la IED puede abordar la metodología que más se adapte a sus necesidades.

3. Plan de capacitación y concientización: debe contener información de las capacitaciones requeridas para implementar la continuidad del negocio, y preservar adecuadamente la seguridad de la información.

4. Copias de seguridad: Lineamientos para la generación y prueba de las copias de seguridad.

5. Servicios de red: Identifica los servicios de red de la IED, usuarios y permisos pertinentes a fin de garantizar la seguridad de la información.

6. Seguridad física y ambiental: define las estrategias para proteger los activos de información de las amenazas naturales y ambientales, por interrupción de servicios públicos, o amenazas artificiales internas o externas.

Nivel 4

Se deben generar los formatos que den cuenta de la evidencia de la seguridad de la información y que hayan sido definidos en la Fase I que se encuentran relacionados en el esquema documental, ver gráfica 56.

5.2.3. Fase III - Implementación

En esta fase la IED debe diseñar y poner en marcha la documentación en todos sus niveles, iniciando por la documentación de Nivel 1 y finalizando con la documentación de Nivel 4.

Se deben realizar las siguientes actividades:

1. Diseñar el esquema documental.
2. Implementar de controles seleccionados del anexo A de la Norma ISO 27001
3. Implementar el plan de tratamiento de riesgos definido.
4. Socialización del SGSI.
5. Capacitación y concientización.
6. Operación del sistema.

5.2.4. **Fase IV – Evaluación de desempeño**

Los indicadores de gestión propuestos para el SGSI, permitirán realizar el seguimiento a la efectividad, eficiencia y eficacia de la seguridad de la información de acuerdo a lo planificado en la Fase I.

En esta fase se realizan las siguientes actividades:

1. Auditoría interna
2. Revisión por la dirección

5.2.5. Fase V – Mejora continua

En esta etapa se revisan los resultados obtenidos en la fase anterior, permitiendo el análisis de causas para las desviaciones o No conformidades encontradas, de tal manera que los planes de mejoramiento se conviertan en acciones contundentes que impidan la repetición de la desviación.

Las acciones tomadas darán cuenta entonces de la desviación en sí misma, el análisis de causas (Para el cual es posible emplear métodos como Cinco Porqué, Árbol de problemas, Ishikawa, etc.), acciones a implementar como tratamiento de la desviación y/o mejoramiento detectado, plan de evaluación de la efectividad de las acciones tomadas.

En esta fase se realizan las siguientes actividades:

1. Análisis de No Conformidades o desviaciones
2. Establecimiento de acciones correctivas

5.2.6. Fase V – Selección de herramienta para la socialización del modelo

Se realizó la investigación de software GNU/GPL disponible que permitiera distribuir y socializar el modelo propuesto en la Secretaría Académica de las IED’s en las cuales se adelantó el proceso de validación, para determinar cuál era la más pertinente, se llevó a cabo un proceso de calificación de acuerdo a los factores de presentados en la tabla 21

Tabla 21. Criterios de calificación de las plataformas GNU/GPL que permiten la distribución y socialización del SGSI

Fuente: propia

CRITERIO	VALOR	DESCRIPCIÓN
Actualización	1	No se ha vuelto a actualizar
	2	Actualizado al menos una vez por año
	3	Actualizado al menos dos veces por año
	4	Actualizado más de dos veces al año
Instalación	1	Instalación manual, a través de comandos
	2	Instalación guiada con requerimientos de conocimientos técnicos
	3	Instalación guiada sin requerimientos de conocimientos técnicos
Facilidad de uso	1	Requiere amplia capacitación para su uso
	2	Requiere inducción sencilla para su uso
	3	Intuitivo y fácil de emplear
Soporte	1	No tiene soporte
	2	Soporte algunos días y por correo electrónico
	3	Soporte todos los días chat, teléfono y correo
Administración	1	No posee módulo de administración
	2	Posee módulo de administración, requiere amplio conocimiento
	3	Posee módulo de administración, no requiere amplio conocimiento
Aplicación WEB	1	No posee aplicación WEB
	2	Solo posee aplicación de escritorio con entorno de red
	3	Posee aplicación WEB
Cumplimiento ISO 27001	1	Permite documentar menos del 25% de requisitos de la Norma
	2	Permite documentar entre el 26% y el 50% de requisitos de la Norma
	3	Permite documentar entre el 50% y el 75% de requisitos de la Norma
	4	Permite documentar entre el 75% y 100% de los requisitos de la Norma
Compatibilidad	1	Solo para plataformas Linux
	2	Solo para plataformas Windows
	3	Permite instalación en plataformas Linux y Windows
Tiempo de respuesta	1	Más de 1 minuto
	2	Entre 40 y 60 segundos
	3	Entre 20 y 40 segundos
	4	Entre 5 y 20 segundos
	5	Menos de 5 segundos
Seguridad	1	No posee seguridad
	2	Seguridad básica solo usuario y contraseña
	3	Altos niveles de seguridad, incluye logs y encriptación

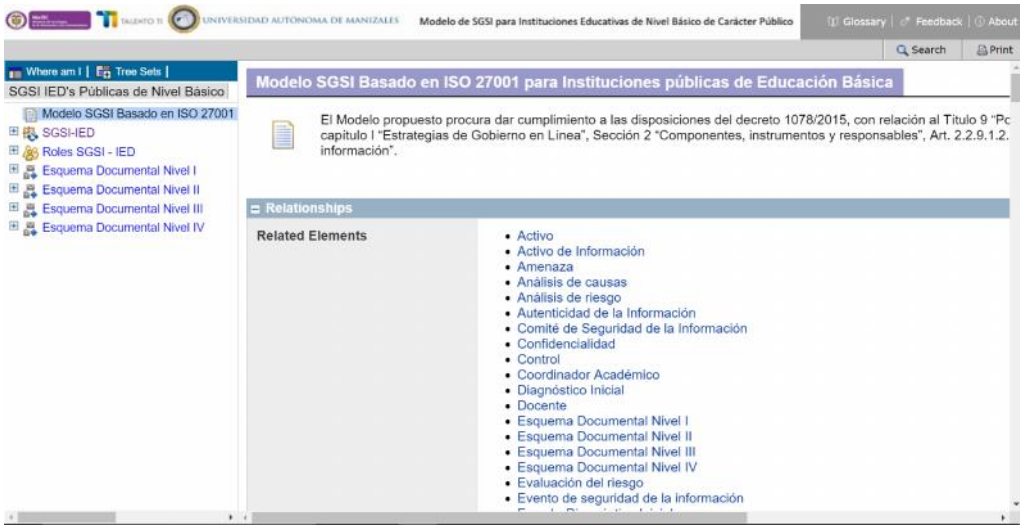
Los resultados obtenidos luego del proceso de evaluación se resumen en la gráfica 57:

SOFTWARE	VER	ACTUALIZACIÓN	INSTALACIÓN	FACILIDAD DE USO	SOPORTE	ADMINISTRACIÓN	APLICACIÓN WEB	CUMPLIMIENTO ISO 27001	COMPATIBILIDAD	TIEMPO DE RESPUESTA	SEGURIDAD	TOTAL
		1-4	1-3	1-3	1-3	1-3	1-3	1-4	1-3	1-5	1-3	
SECURIA SGSI	1,2,4	2	3	1	2	2	1	3	2	3	2	21
FRAMBA	Community	3	1	1	2	2	3	3	1	4	3	23
EPE - COMPOSER	1,1,1,8	2	3	2	3	3	3	4	3	4	1	28

Gráfica 57. Selección de software GNU/GPL distribución SGSI.

Fuente: Propia

El puntaje más alto lo obtuvo el software EPF – Composer, por lo que se generó un plugin, basado en la plantilla publicada en The Eclipse Foundation para Scrum de tal manera que se facilitó la socialización web del modelo propuesto en las Secretarías de Educación en las cuales se llevó a cabo el proceso de validación



Gráfica 58. PlugIn EpfComposer basado en Scrum para la socialización del modelo de SGSI propuesto

Fuente: Propia

5.3.Validación del modelo

5.3.1. Identificación de riesgos en las IED's de validación

La validación se llevó a cabo en una de las IED de la Comuna Universidad y una IED de la Comuna San Fernando de la Ciudad de Pereira respectivamente, para realizar este proceso se desarrollaron los siguientes pasos:

Paso 1 Determinación del Alcance: Secretaria Académica de las IED's.

Paso 2 Inventario de Activos: se realizó la identificación de los activos del área de la secretaria académica existentes en las IED's tomando como referencia los identificados en el modelo, teniendo como resultados los mostrados en la siguiente tabla:

Tabla 22. Validación inventario de activos

Fuente: Propia

NO ACTIVO	TIPO ACTIVO	DESCRIPCIÓN	OBSERVACIONES	IED's	
				1	2
1	Físico	Archivador	Almacenamiento de carpetas de los estudiantes, información de los docentes, certificados académicos, soportes escolares	x	x
2	Tecnológico	Computador	Registro de información académica en el software institucional y en el SIMAT, generación de certificados académicos y elaboración de informes	x	x
3	Tecnológico	Impresora	Impresión de los certificados de estudio, informes de rectoría, constancias	x	x
4	Tecnológico	Estabilizador	Protección del equipo para el procesamiento de información académica	x	X
5	Tecnológico	Teléfono	Atención al público, comunicación interna y externa	x	X
6	Humano	Secretaria Académica	Persona responsable del manejo y administración de la información de carácter académico de los estudiantes y soportes de desarrollo profesional de los docentes	x	X
7	Físico	Carpetas de soportes académicos de los estudiantes	Almacenamiento del historial académico de los estudiantes, desde la matrícula hasta el último año cursado	x	X
8	Físico	Carpetas con soportes de cualificación profesional y hoja de vida de los docentes	Almacenamiento de hojas de vida de los docentes y los soportes del desarrollo profesional	x	X
9	Físico	Oficina de Secretaría Académica	Lugar en el cual se llevan a cabo todas las actividades académicas y de almacenamiento de información física y digital	x	X
10	Lógico	Software de control académico	Programa de computadora que emplea la IED para administrar la información de los estudiantes, matriculas, asignación de grupos, docentes, registro de calificaciones, etc	x	X
11	Lógico	Sistema Operativo	Base operativa del equipo para el procesamiento de la información	x	X
12	Lógico	Paquete ofimático	Procesadores de texto, presentación en diapositivas, hojas de cálculo	x	X
13	Proceso	Matrícula	Registro de los estudiantes en el software de la IED y reporte en el SIMAT	x	X

NO ACTIVO	TIPO ACTIVO	DESCRIPCIÓN	OBSERVACIONES	IED's	
				1	2
14	Proceso	Actualización información docente	Actualización de los soportes de estudios de los docentes de la IED en su respectiva carpeta	x	X
15	Proceso	Emisión de certificados	Generación e impresión de certificados de notas y de estudio	x	X
16	Proceso	Registro de notas	Registro en el software de la IED de las notas de los estudiantes	x	X
17	Proceso	Generación de informes académicos	Creación y cruce de información para ser presentada en las reuniones de rectoría	x	X
18	Proceso	Generación de actas de grado	Creación de los listados de estudiantes para graduación y actas de grado	x	X
19	Físico	Unidad almacenamiento externo	Unidad para transportar información fuera de la oficina de la secretaría académica	x	X
20	Físico	Conexión de red PC Ethernet	Conexión de red para compartir archivos y acceso a internet	x	X
21	Humano	Rector	Persona responsable de adecuado funcionamiento del proceso de la IED	x	X

Al realizar el análisis de los activos en las dos instituciones se encontró que existe un 100% de coincidencia entre los activos tipo identificados en el modelo y los existentes en los sujetos de validación.

Paso 3 Factores de criticidad de los activos: se emplearon los mismos factores que se tuvieron en cuenta para el análisis de riesgos de los sujetos de estudio del modelo.

Paso 4 Niveles de criticidad de los activos: se aplicaron los mismos niveles que se tuvieron en cuenta para el análisis de riesgos de los sujetos de estudio del modelo, obteniendo resultados similares.

Paso 5 Escenarios de riesgo: La tabla 23 resume los escenarios de riesgos identificados en los sujetos de validación en relación a los activos y a los riesgos tipo identificados en los sujetos de estudio del modelo.

Tabla 23. Validación escenarios de riesgo

Fuente: Propia

No	ESCENARIO DE RIESGO	IED's	
		1	2
1	Afectación legal por pérdida de información del computador de la Secretaría Académica de la IED que almacena la información de los estudiantes y contiene los registros y formatos de las actas de grado y certificados de estudio	X	X
2	Afectación legal por pérdida de la información de los estudiantes y/o docentes por deficiencias en los procesos de inducción y capacitación de la Secretaria Académica de la institución	X	X
3	Afectación legal por pérdida mediante sustracción de las carpetas que contienen los soportes académicos de los estudiantes	X	X
4	Afectación legal por pérdida mediante sustracción de las carpetas que contienen los soportes de cualificación profesional de los docentes	X	X
5	Afectación legal por pérdida de la información del software de control académico de la Institución	X	X
6	Afectación legal por errores en el proceso de matrícula al registrar la información de los estudiantes en el software de la IED y /o en el SIMAT, por parte de personal no idóneo o con falta de entrenamiento	X	X
7	Acceso a información confidencial de los estudiantes y/o docentes mediante fotografías o copias no autorizadas de las carpetas almacenadas en el archivo, empleando dispositivos móviles por falta de control en el acceso al mismo	X	X
8	Acceso a información confidencial mediante la sustracción de información del computador de la secretaría académica empleando conexión no autorizada a través de dispositivos móviles o unidades de almacenamiento extraíble	X	X
9	Acceso a información confidencial de los estudiantes a través de dispositivos móviles durante el proceso de registro de calificaciones en el software de la IED, por exposición del escritorio de trabajo de la secretaria académica a personal no autorizado	X	X
10	Acceso a información confidencial mediante la interceptación de la red interna de la secretaría académica a través del cableado del cielo raso que queda expuesto fuera de las oficinas por falta de mecanismos de protección	X	X
11	Tratamiento erróneo de la información de los estudiantes en el software de control de la IED y/o en el SIMAT afectando los reportes requeridos por la Secretaría de Educación y los informes a la rectoría por falta de entrenamiento del personal	X	X
12	Alteración de la información académica de los estudiantes por errores en el tratamiento de la información por parte del software de control académico de la IED	X	X
13	Alteración del proceso de generación de actas de grado, mediante la expedición errónea y/o no autorizada de actas con sello de la institución con participación del personal de la secretaría académica	X	X
14	Divulgación no autorizada por parte del personal de la secretaría académica de la información de personal de los estudiantes y/o docentes a terceros	X	X
15	Tratamiento erróneo de la información de los estudiantes y/o docentes tanto digital como física por deficiencias en los canales de comunicación de las políticas administrativas establecidas por el rector de la institución	X	X
16	Acceso no autorizado al área de archivo de las carpetas con la información de los estudiantes y/o docentes de la IED, por falta de mecanismos de control de acceso de personal externo	X	X
17	Acceso no autorizado al computador del área de secretaría académica por falta de mecanismos de control de acceso a personal externo y/o falta de control en la atención al público	X	X
18	Acceso no autorizado al software de control académico por ausencia de mecanismos de control en el puesto de trabajo de la secretaria académica	X	X
19	Acceso no autorizado al proceso de matrícula de los estudiantes en el software de la IED y/o al SIMAT por ausencia de políticas sobre el manejo confidencial de la información de registro académico	X	X
20	Acceso no autorizado al proceso de registro de calificaciones de los estudiantes en el software de la IED por ausencia de políticas sobre el manejo confidencial de la información de registro académico	X	X
21	Acceso no autorizado a las plantillas institucionales para la generación de actas de grado por falta de controles para el uso del computador de la secretaría académica	X	X

No	ESCENARIO DE RIESGO	IED's	
		1	2
22	Acceso no autorizado a información física y/o digital de los estudiantes y docentes por falta de políticas de acceso para personal no autorizado a la Institución y al área de secretaría académica por parte del rector	X	X
23	Acceso a información confidencial física y/o digital de estudiantes y docentes por parte de los ex colaboradores de la institución por falta de controles para la eliminación de usuarios y políticas de acceso a la planta física de personal retirado de la institución	X	X
24	Errores en el tratamiento de información por ausencia de entrenamiento y/o instrumentos de consulta que permitan que el nuevo personal del área de secretaría académica consulte las particularidades de los procesos adelantados con la información de estudiantes y docentes, tanto en el manejo del archivo físico como en el software de la IED por falta de exigencia de la rectoría en la entrega adecuada del puesto de trabajo por parte de los funcionarios retirados, así como la solicitud de manuales que permitan saber las actividades propias del proceso	X	X
25	Hurto de dispositivos de almacenamiento, procesamiento y/o impresoras del área de secretaría académica por falta de controles de acceso a la IED y al área en horarios de atención al público	X	X
26	Fallos en el equipo de cómputo de la secretaría académica por uso inadecuado del recurso por parte del personal del área	X	X
27	Averías en el equipo de cómputo de la secretaría académica por falta de mantenimiento preventivo programado por la rectoría	X	X
28	Averías en el equipo de cómputo de la secretaría académica por el no reporte oportuno de las incidencias por parte de la secretaria académica	X	X
29	Demora en la atención de los usuarios por problemas de tiempo en el procesamiento de información del equipo de cómputo de la secretaría académica	X	X
30	Demora en la atención de los usuarios por problemas relacionados con la idoneidad en el manejo del equipo de cómputo y/o software para el control académico de la IED por parte de la secretaria académica	X	X
31	Demora en el proceso de atención de los usuarios por desconocimiento e idoneidad para adelantar el proceso de matrícula de los estudiantes	X	X
32	Demora en el proceso de atención de los usuarios por retraso en el proceso de ingreso de las calificaciones reportadas por los docentes al sistema de control de la IED por parte de la secretaria académica	X	X
33	Demora en el proceso de atención a los usuarios por citaciones a reuniones constantes en horarios habilitados para atención al público por parte del rector	X	X
34	Entrega de plantillas institucionales a personal no autorizado por parte de la secretaria académica	X	X
35	Fallos o demoras en la atención del público por afectación de software malicioso en el equipo de cómputo de la secretaría académica	X	X
36	Afectación del equipo de la secretaría académica por software malicioso a causa del uso inadecuado del recurso por parte del personal de la secretaría académica	X	X
37	Afectaciones de las comunicaciones por infección de software malicioso que incide en los drivers de la tarjeta de red del computador de la secretaría académica	X	X
38	Pérdida del archivo físico de los estudiantes y docentes por ocurrencia de desastre natural (terremoto, derrumbe, inundación, etc.)	X	X
39	Pérdida del equipo de cómputo e información digital de la secretaría académica por ocurrencia de desastre natural (terremoto, derrumbe, inundación, etc.)	X	X
40	Pérdida de las comunicaciones para el reporte a la Secretaría de Educación y/o entidades externas por daños en los sistemas de comunicación ocasionados por desastres naturales	X	X
41	Pérdida de información en el equipo de cómputo de la secretaría académica por fallos del fluido eléctrico	X	X
42	Daño en el software de control académico por fallos en el fluido eléctrico	X	X
43	Parálisis del proceso de matrícula por fallos en el fluido eléctrico	X	X
44	Retrasos en el proceso de ingreso de calificaciones por fallos en el fluido eléctrico	X	X
45	Daño en el archivo y/o equipos de cómputo e información digital por fuego provocado	X	X

No	ESCENARIO DE RIESGO	IED's	
		1	2
46	Afectación física en el personal del área de secretaría académica por fuego provocado y ausencia de planes de emergencia y/o rutas adecuadas de evacuación	X	X
47	Deterioro del archivo físico de los estudiantes y los docentes por corrosión provocada por humedad	X	X
48	Incumplimiento en los reportes al SIMAT, a la plataforma del ICFES para las pruebas SABER y Secretaría de Educación por fallos en los dispositivos que permiten la prestación del servicio de Internet	X	X
49	Interceptación de datos de los estudiantes por infección con software espía por deficiencias en los mecanismos de protección tales como antivirus y antimalware	X	X
50	Divulgación de la información de los estudiantes y/o docentes por medio de la práctica inadecuada de desecho de información reciclada por parte de la secretaria académica	X	X
51	Divulgación de la información de los estudiantes y/o docentes por falta de políticas y mecanismos para la adecuada disposición de los desechos	X	X
52	Fallos en el funcionamiento del equipo de cómputo de la secretaría académica por instalación de software pirata, ocasionado por falta de políticas con los proveedores, y el personal de la IED	X	X
53	Divulgación y daño en la información confidencial de los estudiantes y/o docentes por retaliaciones políticas en periodos de elecciones por falta de políticas de confidencialidad	X	X
54	Exposición de las contraseñas de acceso a los equipos de cómputo y sistemas de información por falta de medidas de prevención, uso adecuado y preservación de las mismas	X	X
55	Demora en el restablecimiento del servicio por fallos relacionados a la extracción de copias de seguridad y pruebas de las mismas	X	X

Se encontró un escenario de riesgo adicional en la IED de la comuna San Fernando:

Pérdida temporal o permanente de la documentación de los estudiantes por equivocaciones tanto en el almacenamiento en el archivo como en la recuperación del mismo, debido a que la IED San Fernando no cuenta con una oficina exclusiva para el área de Secretaria Académica, compartiendo el espacio de atención y almacenamiento de documentación con el área de Tesorería.

El 100% de los riesgos tipo identificados en la Comuna Universidad, fueron identificados en la Comuna San Fernando.

5.3.2. **Análisis de resultados**

Luego del proceso adelantado, se puede afirmar que el modelo propuesto cumple con los requisitos exigidos por la norma NTC ISO/IEC 27001:2013 necesarios para el establecimiento del

SGSI en las instituciones educativas de nivel básico del sector público, así como las disposiciones establecidas por el MINTIC en la estrategia de gobierno en línea y las disposiciones del MEN en cuanto al cuidado y preservación de los sistemas de información y la calidad del servicio educativo.

Los riesgos identificados en los cuatro sujetos de estudio pertenecientes a la Comuna Universidad, son similares en los sujetos de validación, sin embargo, es importante resaltar que en el proceso de validación adelantado se encontró que el Sujeto de Validación de la Comuna San Fernando comparte el espacio del área de Secretaria Académica con el área de Tesorería, en una oficina de tamaño reducido y en la cual se atiende público de ambas áreas, generando riesgos adicionales a los identificados en los sujetos de estudio; por lo anterior es importante tener presente que los riesgos se incrementan en virtud a la infraestructura y recursos de los que disponga la IED, los cuales están ligados a la cantidad de estudiantes atendidos y ubicación urbana o rural.

Las IED no efectúan procesos de contratación y nombramiento provisionales por lo que es importante que se articulen con la Secretaría de Educación correspondiente o el personal encargado de las convocatorias del Banco de la Excelencia con el fin de identificar y garantizar las competencias necesarias del personal para el desarrollo de sus funciones, acordes con los sistemas de información que se manejan en las instituciones.

Las IED’s emplean controles enfocados en la prevención de la probabilidad de ocurrencia, pero descuidan drásticamente la implementación de controles tendientes a la mitigación del impacto de la materialización de los riesgos.

Es importante realizar un análisis de los riesgos asociado a las características particulares de las IED’s con el fin de cubrir el 100% de las vulnerabilidades institucionales asociadas a temas de mejoramiento y sostenibilidad de su infraestructura, dado que la Declaración de Aplicabilidad se generó a partir de los riesgos comunes encontrados en los sujetos de estudio, quienes tienen

heterogeneidad de estudiantes en cuanto a los niveles sociales atendidos, y los recursos aprobados para su funcionamiento por parte de la Secretaria de Educación.

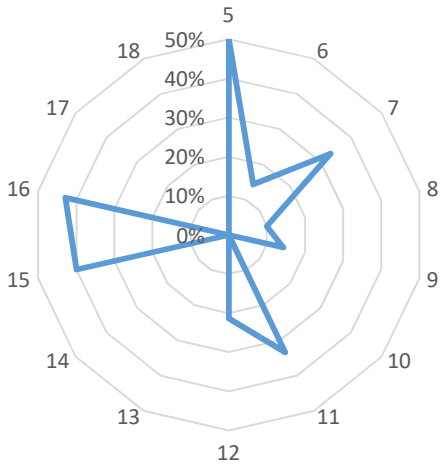
Es necesario planificar un proceso de concientización y socialización de los riesgos a los cuales se encuentran expuestos las instituciones educativas, no solo con la planta de personal propia de la IED, sino también con las Secretarias de Educación y el Ministerio de Educación a fin de encaminar estrategias tenientes a disminuir la brecha existente en matería de seguridad de la información.

La tabla 24, resume la variación en la adopción de controles del anexo A de la norma NTC ISO/IEC 27001:2013 con respecto de los que actualmente se tienen implementados en las IED's.

Tabla 24 Tabla comparativa de la adopción de controles encontrados en los sujetos de estudio, los incluidos en el plan de mitigación y los planteados en el modelo propuesto

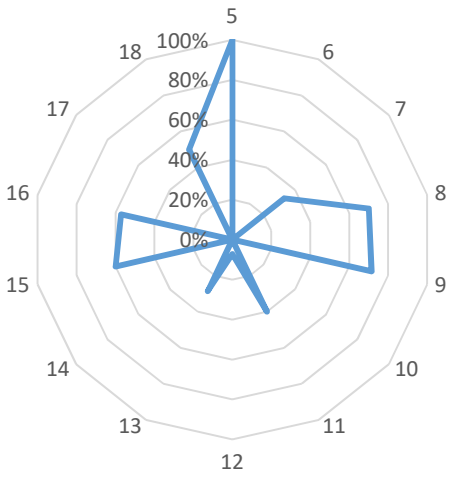
DOMINIO	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**TC**
#Controles	**2**	**7**	**6**	**10**	**14**	**2**	**15**	**14**	**7**	**13**	**5**	**7**	**4**	**8**	**114**
#Ctrl Actuales	1	1	2	1	2	0	5	3	0	0	2	3	0	0	20
%Adop, Ctrl Act.	50	14	33	10	14	0	33	21	0	0	40	43	0	0	18
#Ctrl Propuestos	2	0	2	7	10	0	6	1	2	0	3	4	0	4	41
%Adop Ctrl Prop.	100	0	33	70	71	0	40	7	29	0	60	57	0	50	36
#Ctrl Modelo	2	1	3	8	11	0	11	4	2	0	5	7	0	4	58
%Adop Ctrl Modelo	100	14	50	80	79	0	73	29	29	0	100	100	0	50	51

Se puede observar que existe un incremento del 33% de los controles adoptados por el modelo propuesto en relación al porcentaje de controles identificados en los sujetos de estudio, las siguientes gráficas resumen los dominios en los cuales se intervino mediante el plan de mitigación de riesgos.



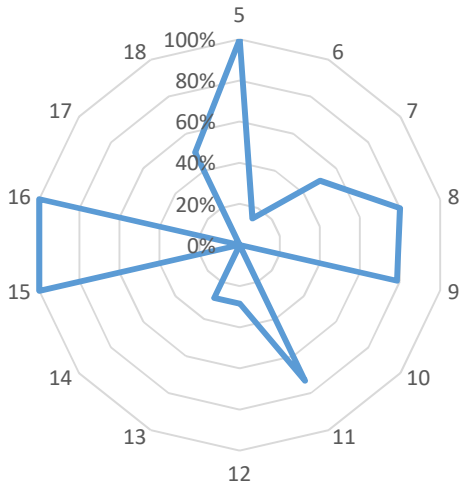
Gráfica 59. Adopción actual de los controles del anexo A de la norma NTC ISO/IEC 27001:2013 en los sujetos de estudio

Fuente: Propia



Gráfica 60. Adopción de los controles del anexo A de la norma NTC ISO/IEC 27001:2013 en el plan de mitigación

Fuente: Propia



Gráfica 61. . Adopción de los controles del anexo A de la norma NTC ISO/IEC 27001:2013 en el modelo propuesto

Fuente: Propia

6. Conclusiones

El establecimiento de un Modelo de Sistema de Gestión de Seguridad de la Información basado en la Norma ISO 27001:2013 para instituciones de educación básica de carácter público, proporciona una línea base para el cumplimiento del Decreto Único Reglamentario 1078/2015 componente “Seguridad y privacidad de la información”, a la vez que permite cumplir con los mandatos emanados por el Decreto 1526, en lo referente a la calidad de la información y la responsabilidad de las entidades territoriales de realizar auditorías por lo menos una vez al año a la población matriculada y a los docentes ayudando a preparar las IED’s para estos procesos de verificación.

De igual manera y acorde a lo estipulado por el Decreto 1377/2013 Art. 7, en el cual se hace referencia a la capacitación sobre la identificación de riesgos en los niños, niñas y adolescentes respecto del tratamiento indebido de la información personal, la aplicación de los controles seleccionados permite disminuir los riesgos que con respecto al particular fueron encontrados en el área de Secretaria Académica.

Existe una falta de entendimiento por parte del personal responsable de la administración, mantenimiento y control de la información de los niños, niñas, adolescentes y docentes sobre el impacto de la materialización de los riesgos de seguridad de la información en términos del impacto.

Las contiendas políticas incrementan los riesgos de exposición de información institucional, particularmente en temporada de elecciones, constituyendo este un riesgo que va en detrimento de la IED y de la información de los niños, niñas, adolescentes, docentes y personal administrativo.

El modelo constituye una base para garantizar la Confidencialidad, la Integridad y la Disponibilidad de la información sensible de niños, niñas adolescentes, docentes y personal administrativo, en procura del cumplimiento de lo dispuesto en el Decreto Único Reglamentario 1075/2015 del Sector Educación, además de fortalecer los indicadores de GEL, a través del cumplimiento de lo dispuesto en el Decreto Único Reglamentario 1078/2015 del Sector TIC componente “Seguridad y privacidad de la información”, alineado con el modelo expuesto por MINTIC que tiene como base la Norma Internacional NTC ISO/IEC 27001:2013.

El modelo de SGSI propuesto, da su aporte social evitando que la información sensible de los niños, niñas y adolescentes sea manipulada por personas inescrupulosas que la emplean con la finalidad de involucrar a los menores en redes de prostitución y pornografía infantil.

El modelo de SGSI constituye una herramienta que genera cultura sobre la disposición de los desechos tecnológicos de las IED’s previniendo que las áreas circundantes se vean contaminadas visual y químicamente por el inadecuado manejo de los activos que han sido dados de baja del inventario.

Los requisitos establecidos por el MEN en materia de seguridad de información, sistemas de información y calidad de la información, son abarcados en un 100% por la estrategia GEL a través del componente “Seguridad y Privacidad de la Información”, ver tabla 25.

Tabla 25. Cumplimiento de requisitos en materia de Seguridad de la Información del MEN por parte de la estrategia GEL

Requisitos MEN en SI	**GEL Componente seguridad y privacidad**	**Modelo Propuesto MINTIC**	**Modelo Propuesto SGSI**
Decreto 1526/2002 "Reglamentación para la administración de los SI del sector educativo", Art 1, "El sistema estará compuesto por información que	OBJ1: Definición de un marco de	Diagnóstico del grado de	Diagnóstico inicial de cumplimiento

permita realizar el monitoreo del servicio educativo y la evaluación de sus resultados"	seguridad de la información y de los sistemas de información. OBJ2: Implementación del plan de seguridad y privacidad de la información y de los sistemas de información. OBJ3: Monitoreo y mejoramiento continuo	madurez del SGSI Análisis y tratamiento de riesgos (Riesgos no identificados en un sector particular) Declaración de aplicabilidad 109 controles, 1 inexistente en el anexo A de la norma ISO 27001:2013 Guías técnicas para documentar el SGSI	de requisitos NTC ISO/IEC 27001:2013 Análisis y tratamiento de riesgos identificados para las IED's de básica de carácter público. Declaración de aplicabilidad, 58 controles del anexo A Norma ISO 27001:2013. Documentación del modelo
Decreto 1526/2002 "Reglamentación para la administración de los SI del sector educativo" ..Art 4, "Características de la calidad de la información y responsabilidad del tratamiento de la misma"			
Ley 1581/2012 "Disposiciones generales para la protección de datos personales".. Art 7 "Es tarea del estado y de las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del tratamiento indebido de sus datos personales"			
Ley 715/2001 "Disposiciones para organizar la prestación de los servicios de educación y salud", Título II, Capítulos 1 al 6			
Ley 115/1994 "Ley general de educación", Art 2			
Resolución 166/2003 "Condiciones para el reporte de información para la implementación de la primera etapa del sistema de información del sector educativo"			
Decreto único reglamentario 1075/2015 del sector educación			

El Modelo propuesto es aplicable a todas las instituciones educativas de nivel básico del sector público.

7. Recomendaciones

Es importante que las instituciones educativas de nivel básico del sector público, establezcan mecanismos que permitan garantizar la idoneidad de las personas que son contratadas y enviadas a la institución educativa, pues debido a la falta de control sobre el proceso de selección se maximizan los riesgos de exposición de información, ya sea de manera deliberada o accidental.

Es de vital importancia que los rectores de las IED, promuevan talleres de concientización y buenas prácticas de seguridad de la información.

A futuro se debería investigar la efectividad de los procesos de selección de personal administrativo por parte de las Secretarias de Educación, así como el impacto de las corrientes políticas en el cubrimiento de los puestos laborales que tienen acceso a la información de niños, niñas, adolescentes y docentes, con el fin de establecer estrategias y controles de selección adecuados tendientes a garantizar la confidencialidad, integridad y disponibilidad de la información.

Los rectores de las IED’s deben fortalecer sus conocimientos en cuestiones relacionadas con los riesgos a los que se ven expuestos los niños, niñas, adolescentes, docentes y personal administrativo ocasionados por el tratamiento indebido de los datos personales, en procura de mejorar la gestión de los recursos necesarios que permitan implementar, mantener y mejorar un SGSI.

Es necesario realizar una verificación de los controles adoptados por parte de la estrategia de GEL, en virtud a que se encontró que el documento Manual de Seguridad y Privacidad de la Información del MINTIC, incluye el código de control 16.2 “Notificación de los eventos de

seguridad de la información", el cual no se encuentra en el anexo A de la norma NTC ISO/IEC 27001:2013.

Se debe investigar a futuro la aplicabilidad del modelo propuesto en instituciones educativas de características similares en otros municipios y departamentos del país, tanto públicas como privadas.

Desarrollar una plataforma web de gestión documental que se adapte a los requerimientos del SGSI basado en NTC ISO/IEC 27001, que tenga presente las características de infraestructura de las IED's.

Incluir dentro de la planta de personal de los IED's un profesional idóneo y responsable del área de tecnología que no cumpla funciones docentes, con la finalidad de garantizar la atención oportuna de los incidentes que se presentan en la IED, además de ser la persona responsable del SGSI.

8. Bibliografía

Aliaga Florez, L. C. (2013). *Diseño de un Sistema de Gestión de Seguridad de Información para un Instituto Educativo.* Lima, Perú.

AS/NZS. (1999). *Estándar Australiano AS/NZS 4360:1999 Administración de riesgos.*

Betancourt Correa, L., Posada Bonilla, D., & Rangel García, C. (2014). *Diseño del sistema de gestión de seguridad de la información (SGSI) para el proceso administrativo de la alcaldía de Manizales.* Tesis, Universidad Autónoma de Manizales, Manizales, Caldas.

Buitrago Estrada, J. C., Bonilla Pineda, D. H., & Murillo Varón, C. E. (2012). *Diseño de una metodologìa para la implementación del sistema de gestión de seguridad de la información SGSI en el sector de laboratorios de análisis mircrobiológicos, basado en ISO 27001*. Universidad EAN, Bogotá.

Caviedes Sanabria, F., & Prado Urrego, B. (2012). *Modelo unificado para identificación y valoración de los riesgos de los activos de información en una organización.* Tesis, Universidad ICESI, Santiago de Cali, Valle del Cauca.

Codesocial. (2009). Organización del Sistema Educativo, Conceptos Generales de la Educación Preescolar, Básica y Media. *Revolución Educativa Colombia aprende*, 11.

Comisión de derechos humanos. (1948). *Declaración universal de los derechos humanos.* Paris, Francia.

Condori Benavides, I. (2015). *Informe de Control Interno II Congreso Nacional de Contabilidad.* Universidad Autónoma del Perú, Lima, Perú.

Constitución Política de Colombia. (1991). *Constitución Política de Colombia.* Bogotá.

Decreto 1078. (2015). *"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".* Bogotá.

Departamento Nacional de Planeación. (2016). *Política nacional de seguridad digital.* Consejo Nacional de Política Económica y Social, Bogotá, Colombia.

Détienne, F., Rouet, J.-F., Burkhardt, J.-M., Deleuze-Dordron, C., Kumar, R., Khan, S., . . . Turnes, L. (2002). Risk Management Guide for Information Technology Systems : Recommendations of the National Institute of Standards and Technology. En N. I. Technology, *Journal of Systems and Software* (Vol. 30, págs. 1-22). Falls Church, VA: Booz Allen Hamilton Inc. doi:10.1111/j.1745-6622.2008.00202.x

Espinosa Betancur, J. G., García Gallo, R. S., & Giraldo Restrepo, A. (2016). *Sistema de gestión de seguridad de la información para los tres procesos misionales de la corporación autónoma regional de risaralda (CARDER).* Manizales, Caldas.

Espinosa T., D., Martinez P., J., & Amador D., S. (02 de 12 de 2014). Gestion del riesgo en la seguridad de la información base en la norma ISO/IEC 27005 de 2011, proponiendo una adaptación de la metología octave-s. *Ing. USBMed, 5*(2), 33-43.

Fernández Martín, I. (2013). *Implantación de la metología BPM en la Eps: Aplicación para la gestión de comisiones.* Alicante.

Garimella, K., Lees, M., & Williams, B. (2014). *BPM - Gerencia de procesos de negocios.*

Grinnel, R. (1997). *Social work research of evaluation: Quantitative and qualitative approaches* (5a. ed.). Itasca, Illinois: Peacock Publishers.

Instituto colombiano de normas técnicas y certificación. (2013). *Norma técnica colombiana NTC-ISO-IEC 27001*. ICONTEC.

Irrazabal, M., Gómez, D., & Cardoso, W. (2013). *SGSI : de la academia a la práctica.* Montevideo, Uruguay: ISACA.

ISACA. (2009). *Marcos de riesgos de TI.* Rolling, meadows.

ISACA. (2012). *COBIT 5 Un marco de negocio para el gobierno y la gestión de las TI de la empresa.* Rolling Meadows, EE.UU. Obtenido de www.isaca.org/COBITuse

ISO. (2009). *Norma ISO 31000 versión 2009: Gestión de riesgos - principios y guías.* Switzerland. Obtenido de www.iso.org

ISO. (2014). *International standard ISO/IEC 27000.* Switzerland: ISO. Obtenido de www.iso.org

ISO/IEC 31000. (2009). *Gestión de RIesgos.* Bogotá.

ISO27000.es. (16 de enero de 2017). *El portal de ISO 27001 en español*. Obtenido de Iso27000.es: http://iso27000.es/iso27002.html

ISO27000.es. (s.f.). *ISO 27000.es*. Obtenido de http://www.iso27000.es/sgsi.html

León Zuluaga, M., & Grajales Valencia , L. (2016). *Diagnóstico del grado de madurez de los controles de seguridad establecidos en la Norma NTC ISO/IEC 27001:2013 para asegurar la confidencialidad, integridad, dispobilidad y control de la información en instituciones públicas de educación preescolar de la.* Pereira, Risaralda.

Ley 115. (1994). *Por la cual se expide la ley general de educación.* Bogotá.

Ley 1581. (2012). *Por lo cual se dictan disposiciones generales para la Protección de Datos Personales.* Bogotá.

Ley 489. (1998). *por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional, se expiden las disposiciones, principios y reglas generales para el ejercicio de las atribuciones previstas en los numerales 15 y 16 del artículo 189.* Bogotá.

Ley 715. (2001). *Por la cual se dictan normas orgánicas en materia de recursos y competencias de conformidad con los artículos.* Bogotá.

M. Talabis, M. R., & L. Martín, J. (2013). *Herramientas para la Evaluación de Riesgos.* United States of America: ELSEVIER.

Ministerio de hacienda y admnistraciones publicas, Gobierno de España. (2012). *MAGERIT - versión 3.0 Metodología de análisis y gestión de riesgos de los sistemas de información.* Dirección general de modernización administrativa procedimientos e impulso de la administración electrónica. Madrid, España: Ministerio de Hacienda y Administraciones Públicas. Obtenido de http://administracionelectronica.gob.es/

Ministerio de la Presidencia. (2010). *Boletín oficial del Estado.* España. Obtenido de https://www.boe.es

Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC. (2015). *Guía encuesta diagnóstico modelo de segureidad de la información para las entidades del estado.* Bogota, Colombia.

Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC. (2015). *Modelo de seguridad y privacidad de la información.* Bogotá, Colombia.

MINTIC. (2015). *Indice de Gobierno en Línea*. Obtenido de Indice de Gobierno en Línea: http://indicegel.gobiernoenlinea.gov.co/Resultados_Sector.aspx

MINTIC. (2015). *Manual estrategia de gobierno en línea.* Bogotá, Colombia. Obtenido de http://estrategia.gobiernoenlinea.gov.co

MINTIC. (2016). *Guía de gestión de riesgos.* Bogotá, Colombia.

Monserrat, S. (2008). La Ecología de la Información: Un nuevo paradigma de la infosfera. *Pliegos de Yuste*(7 - 8).

Muñoz, M. (2013). Introduccion Octave. En S. E. Institute, *Journal of Chemical Information and Modeling* (págs. 1689-1699). Carnegie Mellon University. doi:10.1017/CBO9781107415324.004

Naciones Unidas. (1976). *Pacto internacional de los derechos económicos, sociales y culturales.*

Novoa, A., & Helena, C. (2015). *Metodología para la Implementación de un SGSI en la Fundación Universitaria Juan de Castellanos, Bajo la Norma ISO 27001:2005.* Tesis, Universidad Internacional de la Rioja, Tunja, Boyacá.

NTC ISO/IEC 27001. (2013). *Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.* Bogotá.

OSI ISO-7498-2. (1989). *Modelo Arquitectura de Seguridad.*

Peña Ibarra, J. (2009). *Metodologías y normas para el análisis de riesgos.* Monterrey. Mexico: ISACA.

Presidencia de la Republica de Colombia. (2002). *Decreto 1526.* Bogotá.

Ramírez Castro, A., & Ortiz Bayona, Z. (2011). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. *Ingeniería*, *16*(2).

Torres Bermúdez, A. (2010). *Introducción a la seguridad informática.* Bogotá, Colombia.

UNICEF Comité Español. (2006). *Convención sobre los derechos del niño.* Madrid, España: Nuevo siglo.

Velásquez Isaza, J. (2015). *Modelamiento de los procesos de auditoría en seguridad de la información asociados a los dominios 6, 8, 13 Y 14 del anexo A de La norma Iso 27001 mediante una herramienta de flujo de trabajo.* Tesis, Universidad Tecnológica de Pereira, Pereira, Risaralda. Obtenido de http://repositorio.utp.edu.co/dspace/bitstream/11059/5118/1/0058V434.pdf