Diagnóstico del grado de madurez de los controles de seguridad establecidos en la norma NTC ISO/IEC 27001:2013 para asegurar la confidencialidad, integridad, disponibilidad y control de la información en instituciones públicas de educación preescolar de la ciudad de Pereira – Comuna Universidad.

Liliana Grajales Valencia & Mónica León Zuluaga

Universidad Católica de Pereira

Facultad de Ciencias Básicas e Ingenierías

Profesionalización Ingeniería de Sistemas y Telecomunicaciones

Pereira

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, disponibilidad y control de la información en instituciones públicas de educación preescolar de la ciudad de Pereira – Comuna Universidad.

Liliana Grajales Valencia & Mónica León Zuluaga

Tesis de Grado para optar al título de Ingeniería de Sistemas y Telecomunicaciones

DIRECTOR

Esp. Carlos Arturo Blandón Jaramillo

Universidad Católica de Pereira

Facultad de Ciencias Básicas e Ingenierías

Profesionalización Ingeniería de Sistemas y Telecomunicaciones

Pereira

2016

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Pereira 13 de mayo, 2016

AGRADECIMIENTO

Agradecemos primero a Dios porque sin su voluntad no estaríamos donde estamos, también a cada uno de los docentes que aportaron un granito de arena aportando sus conocimientos y enseñanzas, a nuestras familias por su apoyo, comprensión y acompañamiento en cada uno de los procesos académicos y por último agradecemos enormemente a nuestro tutor Carlos Arturo Blandón Jaramillo, por todo su apoyo, acompañamiento, por creer en nosotras y aportar en nuestro desarrollo personal y profesional

RESUMEN

El avance vertiginoso de las tecnologías de información y su inclusión en las organizaciones tanto de carácter privado como público, así como los riesgos inherentes que subyacen al implementarlas en la cotidiana operatividad de los procesos (estratégicos, misionales y de apoyo) han conllevado a que el Gobierno Nacional y el Ministerio de Tecnología de Información y Comunicación implementen estrategias como Gobierno en Línea con las cuales persigue cerrar las brechas en materia de seguridad de la información que existen en la actualidad en las instituciones del estado (Numeral 1, actividad 4 **"implementar un sistema de gestión de seguridad de la información"),** Los establecimientos educativos del sector público deben en consecuencia implementar un Sistema de gestión de seguridad de la información (SGSI) que les permitan caracterizar y controlar adecuadamente los riesgos asegurando la confidencialidad, la integridad y la disponibilidad de la información.

Por esta razón está tesis pretende diagnosticar el grado de madurez de los controles de seguridad establecidos en la norma NTC ISO/IEC 27001:2013 para instituciones públicas de educación preescolar de la comuna universidad de la ciudad de Pereira.

Palabras clave: información, seguridad, Integridad, confidencialidad, disponibilidad, controles, seguridad de la información

ABSTRACT

The breathtaking progress of information technologies and its incorporation in public and private organizations, this way as inherent risks that underlying on implement them in the daily operability of the processes (strategic, missionary and of support) have led to the National Government and the Ministry of Information Technology and Communication implement strategies such on-line government which try to close the gaps about information safety that exist at present in the state institutions (Numeral 1, activity 4 " to implement a management system information safety "), Educational institutions in the public sector should implement System Management Information Safety (SMIS) That allow them to characterize and to control the risks assuring confidentiality, integrity and the availability of the information.

For this reason, this project attempts to diagnose the maturity degree of the safety controls established in the norm NTC ISO/IEC 27001:2013 for public institutions of pre-school education of the commune university city of Pereira.

Keywords: information, security, integrity, confidentiality, availability, controls, Security of the information

TABLA DE CONTENIDO

INTRODUCCIÓN 13
1. FORMULACIÓN DEL PROYECTO 14
1.1 DESCRIPCIÓN Y FORMULACIÓN DEL PROBLEMA 14
1.2 OBJETIVO GENERAL 14
1.2.1 Objetivos Específicos 14
1.3 JUSTIFICACIÓN 15
1.4 PLANTEAMIENTO DE HIPÓTESIS 18
1.5 IDENTIFICACIÓN DE VARIABLES 19
1.6 PRESUPUESTO 19
1.7 CRONOGRAMA 22
2. MARCO CONTEXTUAL. 23
2.1 EL ENTORNO ESCOLAR 23
2.2 MARCO LEGAL DEL ENTORNO ESCOLAR RELACIONADO CON LA SEGURIDAD DE LA INFORMACIÓN 28
2.3 IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN EN EL ENTORNO ESCOLAR 31
2.4 DIRECTRICES Y LINEAMIENTOS DEL MINISTERIO DE EDUCACIÓN NACIONAL 33
2.5 ESTRUCTURA DE UN ESTABLECIMIENTO EDUCATIVO 34
3. MARCO TEÓRICO 35
3.1 INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN 35
3.1.1 Activo de información 35
3.1.2 Riesgo 36
3.2 SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 37
3.3 DIFERENCIAS ENTRE SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD INFORMÁTICA. 39
3.4 CRITERIOS DE SEGURIDAD DE LA INFORMACIÓN 40
3.5 FAMILIA DE NORMAS ISO/IEC 27000 41
3.6 PRINCIPALES NORMAS A UTILIZAR 43
3.6.1 Norma ISO/IEC 27001 43
3.6.2 Norma ISO/IEC 27001 44
3.6.3 Norma ISO/IEC 31000 45

3.7 REQUERIMIENTOS EXIGIDOS POR LA ISO/IEC 27001 47
3.8 METODOLOGÍAS DE RIESGOS COMO BASE DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 49
3.8.1 NTC ISO 31000 49
3.8.2 ISO/IEC 27005 51
3.8.3 Metodología de riegos de MINTIC 54
3.8.4 CONTROLES ESTABLECIDOS EN LA ISO/IEC 27002. 55
3.9 MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 56
4. MODELO TEÓRICO 59
5. INFORME DE RESULTADO 64
5.1 ANÁLISIS DEL MARCO LEGAL DE LA EDUCACIÓN EN COLOMBIA 64
5.2 DIAGNÓSTICO DEL ESTADO ACTUAL DE LAS INSTITUCIONES EDUCATIVAS DE EDUCACIÓN PREESCOLAR DE LA COMUNA UNIVERSIDAD 66
5.3 DETERMINACIÓN DEL ALCANCE 79
5.4 ESTRUCTURA ORGANIZACIONAL DE LA SEGURIDAD DE LA INFORMACIÓN 80
5.5 IDENTIFICACIÓN DE ACTIVOS TECNOLÓGICOS 81
5.6 DETERMINACIÓN DE RIESGOS 88
5.7 CALIFICACIÓN DEL RIESGO INHERENTE 91
5.8 MAPA DE RIESGO INHERENTE 101
5.9 DEFINICIÓN DE CONTROLES 106
5.10 CALIFICACIÓN DEL RIESGO RESIDUAL 118
5.11 MAPA DE RIESGOS RESIDUAL 128
5.12 PLAN DE MITIGACIÓN DE RIESGOS 133
5.13 DECLARACIÓN DE APLICABILIDAD 155
CONCLUSIONES 205
RECOMENDACIONES 206
REFERENCIAS BIBLIOGRAFICAS 207
GLOSARIO 209

LISTA DE TABLAS

Tabla 1: Presupuesto del proyecto global Fuente: Propia – 2016 19
Tabla 2: Presupuesto detalles de gastos personales Fuente: Propia – 2016 19
Tabla 3: Presupuesto detalles gastos de viaje Fuente: Propia - 2016 20
Tabla 4: Presupuesto detalles inversiones Fuente: Propia – 2016 20
Tabla 5: Presupuesto detalles de gastos generales Fuente: Propia - 2016 21
Tabla 6: Presupuesto detalles servicios técnicos Fuente: Propia - 2016 21
Tabla 7: Descripción detallada de las actividades a realizar durante el proyecto. . 22
Tabla 8. Tabla para interpretación de resultados fase planeación – límites nivel inicial/gestionado. Fuente: MINTIC, 2015 67
Tabla 9. Tabla para interpretación de resultados fase de implementación – límites nivel definido. Fuente: MINTIC, 2015 68
Tabla 10. Tabla para la interpretación de resultados fase de gestión – límites para el nivel gestionado cuantitativamente. Fuente: MINTIC, 2015 69
Tabla 11. Tabla para la interpretación de resultados fase de mejora continua – límites para el nivel optimizado. Fuente: MINTIC, 2015 70
Tabla 12. Fase planeación – nivel inicial/gestionado - valores posibles por pregunta y totales. Fuente MINTIC, 2015 71
Tabla 13. Fase de implementación – nivel definido. Valores posibles por pregunta y totales. Fuente: MINTIC, 2015 73
Tabla 14. Fase de gestión – nivel gestionado cuantitativamente. Valores posibles por pregunta y totales. Fuente: MINTIC, 2015 75
Tabla 15. Fase de mejora continua – nivel optimizado. Valores posibles por pregunta y totales. Fuente: MINTIC, 2015 76
Tabla 16 Resultado del grado de madurez de las instituciones de la comuna universidad Fuente: Propia 78
Tabla 17 Alcance del SGSI de la Institución Fuente: Propia 79
Tabla 18 Factores determinando la criticidad de los activos Fuente propia 81
Tabla 19 Nivel de criticidad de los activos de la información Fuente propia 82

Tabla 20 Criticidad de los activos Fuente propia 83
Tabla 21 Escenario de Riesgo Fuente Propia 88
Tabla 22 Calificación de probabilidades Fuente Propia 91
Tabla 23 Calificación de impacto potencial Fuente NIST SP 800-60 (2008) 92
Tabla 24 Escenarios de riesgos Fuente Propia 94
Tabla 25 Criterios de aceptabilidad del riesgo inherente Fuente propia 101
Tabla 26 Mapa de riesgos confidencialidad inherente Fuente Propia 102
Tabla 27 Mapa de Riesgos Integridad inherente Fuente Propia 103
Tabla 28 Mapa de riesgos disponibilidad inherente Fuente Propia 104
Tabla 29 Mapa de riesgos total inherente Fuente Propia 105
Tabla 30 Definición de controles Fuente Propia 106
Tabla 31 Criterios para la calificación de probabilidades Fuente Propia 118
Tabla 32 Criterios del Impacto potencial Fuente NIST SP 800-60 (2008) 119
Tabla 33 Escenario de riesgos Fuente Propia 120
Tabla 34 Criterios de aceptabilidad del riesgo residual Fuente Propia 128
Tabla 35 Mapa de riesgos confidencialidad residual Fuente Propia 129
Tabla 36 Mapa de riesgo integridad residual Fuente Propia 130
Tabla 37 Mapa de riesgo disponibilidad residual Fuente Propia 131
Tabla 38 Mapa de riesgos total residual Fuente Propia 132
Tabla 39 Plan de mitigación de riesgos Fuente Propia 133
Tabla 40 Controles de declaración de aplicabilidad Fuente Propia 155
Tabla 41 Políticas de la seguridad de la información Fuente Propia 156

LISTA DE GRÁFICAS

Gráfica 1: Representación de la estructura educativa en Colombia – Fuente: elaboración propia 15
Gráfica 2: Representación de los avances de las entidades en la ejecución de la estrategia GEL de orden Nacional Fuente: Índice de Gobierno en Línea..... 16
Gráfica 3: Representación de los avances de las entidades en la ejecución de la estrategia GEL de orden Territorial Fuente: Índice de Gobierno en Línea 17
Gráfica 4 Representación de la posición de los Departamentos, frente a la implementación de GEL Fuente: Índice de Gobierno en Línea 17
Gráfica 5: Representación de los avances de las entidades en la ejecución de la estrategia GEL del departamento de Risaralda Fuente: Índice de Gobierno en Línea 18
Gráfica 6: Múltiples iteraciones circulo de Deming. Fuente: Christoph Roser at AllAboutLean.com..... 32
Gráfica 7: Circulo de riesgos Fuente: http://www.iso27000.es/sgsi.html 38
Gráfica 8: Pilares de la seguridad de la información fuente propia..... 41
Gráfica 9: Circulo de Deming aplicado al SGSI, basado en NTC ISO/IEC 27001. 44
Gráfica 10:Proceso De Gestión Del Riesgo. Fuente: http://www.avantium.es/index.php/gestion-de-riesgos-iso-31000..... 46
Gráfica 11: Sistemas de Gestión de Seguridad de la Información, Fuente: Ana Cecilia Vargas y Alonso Castro Mattei http://archivo.ucr.ac.cr 49
Gráfica 12: Mapa de Análisis de Riesgos bajo la norma ISO/IEC 27005. Fuente. ISO (International Standard Organization) 52
Gráfica 13: Controles establecidos en norma ISO 27002. Fuente ISO/IEC 27002:2013..... 55
Gráfica 14 Niveles de Madurez Fuente Modelo de Seguridad y Privacidad de la Información MINTIC..... 56

Gráfica 15 requerimientos y metas de cada uno de los niveles de grado de madurez Fuente Modelo de Seguridad y Privacidad de la Información MINTIC....57
Gráfica 16 Paralelo entre los niveles y los controles del modelo de seguridad y privacidad de la información Fuente Modelo de Seguridad y Privacidad de la Información MINTIC....58
Gráfica 17 Modelo Teórico. Fuente: Propia....59
Gráfica 18 Resultado del Test de penetración en los equipos del área administrativa de la IED sujeto de estudio. Fuente: Propia 62
Gráfica 20 Descripción del marco legal en Colombia, fuente: propia 65
Gráfica 21. Representación de los tópicos analizados en la valoración de la fase de planeación – Fuente: elaboración propia. 72
Gráfica 22. Representación de los tópicos analizados en la valoración de la fase de implementación – Fuente: elaboración propia....74
Gráfica 23. Representación de los tópicos analizados en la valoración de la fase de gestión – Fuente: elaboración propia 75
Gráfica 24. Representación de los tópicos analizados en la valoración de la fase de mejora continua – Fuente: elaboración propia 76
Gráfica 25 Resultado promedio del diagnóstico realizado a las IEDS Fuente: Propia 77
Gráfica 26 Estructura organizacional de la seguridad de la Información Fuente: Propia 80

INTRODUCCIÓN

El desarrollo desmesurado de las Tecnologías de Información, tanto a nivel de hardware como de software, la incursión de las organizaciones públicas y privadas en un mundo globalizado además de los tratados de libre comercio, exigen niveles de cualificación y de competitividad cada vez mayores, presionando a los diferentes procesos organizacionales a rendir informes en menos tiempos, de mayor calidad y a brindar mayor transparencia en su actuar, pero al entrar en ese mundo globalizado de la tecnología, también se corre el riesgo de exponer a la organización en un mundo de corrupción e inseguridad colocando en peligro el activo más importante "la información".

Como parte de las estrategias para mitigar la corrupción y asegurar la integridad, confiabilidad y seguridad de la información, en el presente trabajo de grado se pretende diagnosticar el grado de madurez de los controles de seguridad de la Información establecidos en la norma NTC ISO/IEC 27001:2013, con el fin de que este proyecto se convierta posteriormente en un punto de partida para el desarrollo de un modelo de sistema de Gestión de Seguridad de la Información que sea aplicable para instituciones públicas de educación preescolar de la ciudad de Pereira – Comuna Universidad.

Durante el proceso de investigación no se han evidenciado documentos que diagnostiquen el grado de madurez de los controles de seguridad de la información y los controles aplicables para instituciones educativas del nivel preescolar, representando esta una oportunidad de mejoramiento para la prestación del servicio educativo y el cierre de brechas en cuanto al cumplimiento de las disposiciones gubernamentales en esta materia.

Para diagnosticar el grado de madurez de los controles de seguridad de la información, se tomaron como sujetos de estudio los colegios públicos de la Comuna Universidad de la Ciudad de Pereira, en los cuales se analizaron los requerimientos establecidos por el Ministerio de Educación en relación con la seguridad de la información en instituciones que presten el servicio de educación preescolar, al igual que las disposiciones emanados del MINTIC a través de los lineamientos establecidos en Estrategias de Gobierno en Línea, en cuanto a la implementación de Sistemas de gestión de Seguridad de la información (SGSI).

1. FORMULACIÓN DEL PROYECTO

1.1 DESCRIPCIÓN Y FORMULACIÓN DEL PROBLEMA

Los establecimientos Educativos de Preescolar de la Comuna Universidad de la Ciudad de Pereira, son Instituciones Públicas del orden territorial, por lo tanto, deben dar cumplimiento al El Decreto 1078 de mayo de 2015 "Por medio del cual se expide el Decreto Único Reglamento del Sector de Tecnologías de la Información y las Comunicaciones", en su Título 9 “Políticas y Lineamientos de Tecnologías de la Información”. Capítulo 1 “Estrategia de Gobierno en Línea”.

1.2 OBJETIVO GENERAL

Diagnosticar el grado de madurez de los controles de seguridad establecidos en la norma NTC ISO/IEC 27001:2013 para asegurar la confidencialidad, integridad, disponibilidad y control de la información en instituciones públicas de educación preescolar de la ciudad de Pereira – Comuna Universidad.

1.2.1 Objetivos Específicos

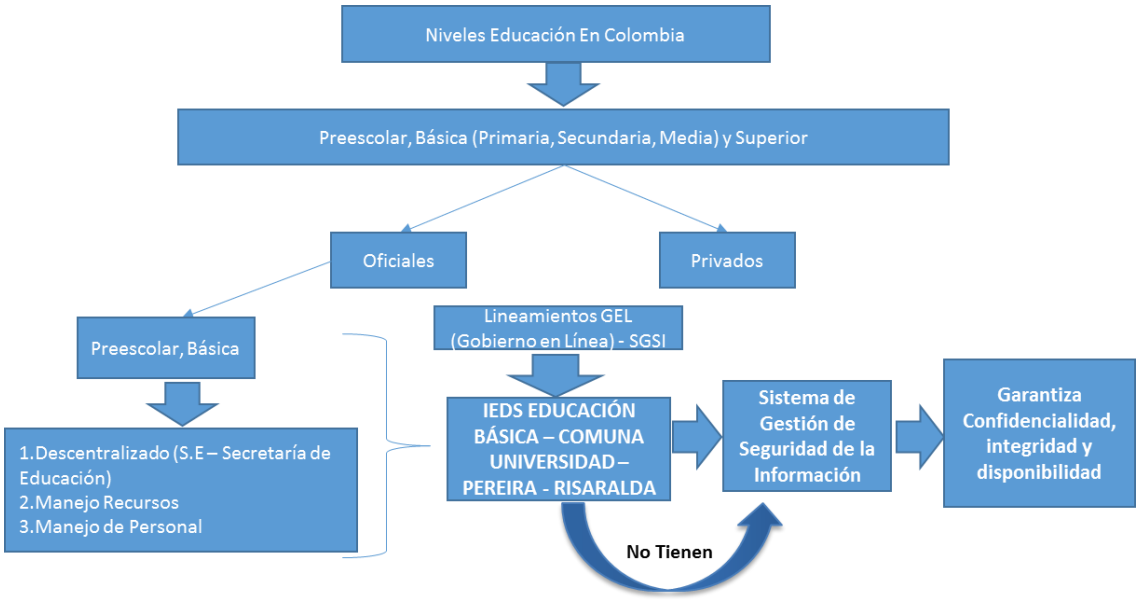
- Analizar los requerimientos del Ministerio de Educación Nacional y las directrices de Gobierno en Línea en torno de la seguridad de la información

- Definir controles asociados a los riesgos de seguridad de información en las instituciones públicas de educación preescolar de Pereira en la comuna Universidad

- Estructurar la declaración de aplicabilidad con base en los controles establecidos en la norma ISO 27001:2013

1.3 JUSTIFICACIÓN

La educación en Colombia se divide en tres niveles: Preescolar, Básica (comprende primaria, secundaria y media) y superior (Codesocial, 2009), los cuales se prestan por instituciones tanto privadas como oficiales. Las instituciones oficiales que prestan el servicio de preescolar tienen como características generales la descentralización, lo que hace que dependan de las secretarias de educación departamentales y municipales tanto para el manejo de los recursos como el manejo de personal. El hecho de ser entidades del orden territorial implica la obligatoriedad de cumplimiento de lo estipulado por el Decreto 1078 de mayo de 2015, en lo indicado en el título 9 con relación a la implementación de un Sistema de Gestión de Seguridad de la Información que garantice la confidencialidad, integridad y disponibilidad de la información, así como la transparencia en la prestación de los servicios y accesibilidad de los ciudadanos.

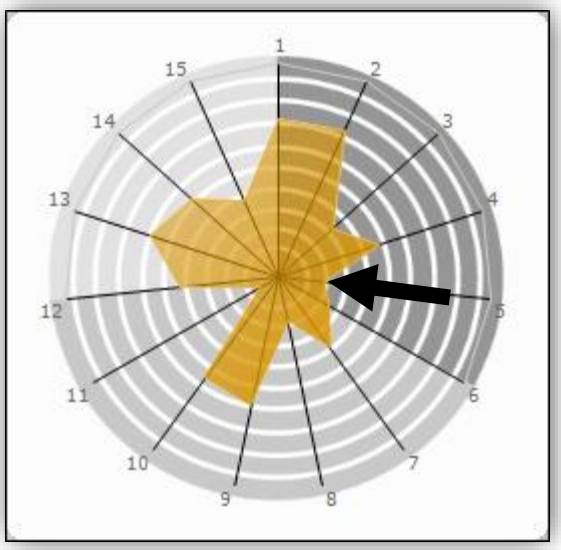


Gráfica 1: Representación de la estructura educativa en Colombia – Fuente: elaboración propia

De acuerdo a los lineamientos de la Estrategia de Gobierno en Línea, en la actividad relacionada número 4 “Implementar un Sistema de Gestión de la Seguridad de la Información”, se requiere el diagnóstico del grado de madurez de los controles de seguridad establecidos en la norma NTC ISO/IEC 27001:2013 para asegurar la confidencialidad, integridad, disponibilidad y control de la información en el ámbito de las instituciones de educación Preescolar, persiguiendo los siguientes beneficios:

- Mejora continua en la gestión de la seguridad
- Disponibilidad del Servicio Educativo
- Reducción de costos de incidentes e inversiones
- Cumplimiento de la legislación
- Incremento de los niveles de confianza de las partes interesadas
- Mejora de la imagen institucional
- Formalización de responsabilidades operativas
- Aseguramiento de la confidencialidad, integridad y disponibilidad de la información

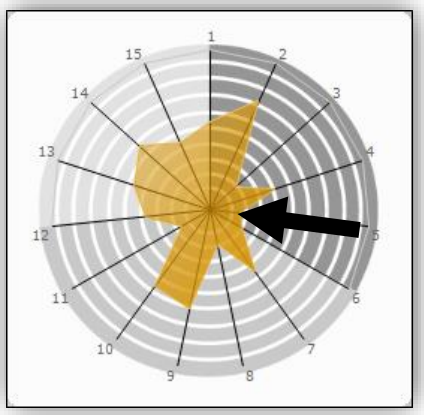
Los índices de GEL del orden nacional revelan que, en el campo educativo, el subíndice Eficiencia Electrónica (Numerales del 1 al 5), tiene un puntaje de 22,05 para la implementación del SGSI (numeral 5) siendo el más bajo de las actividades relacionadas al sub índice (Ver gráfica 2 tomado de (GEL, 2015) Recuperado el día 4 de mayo de 2016)



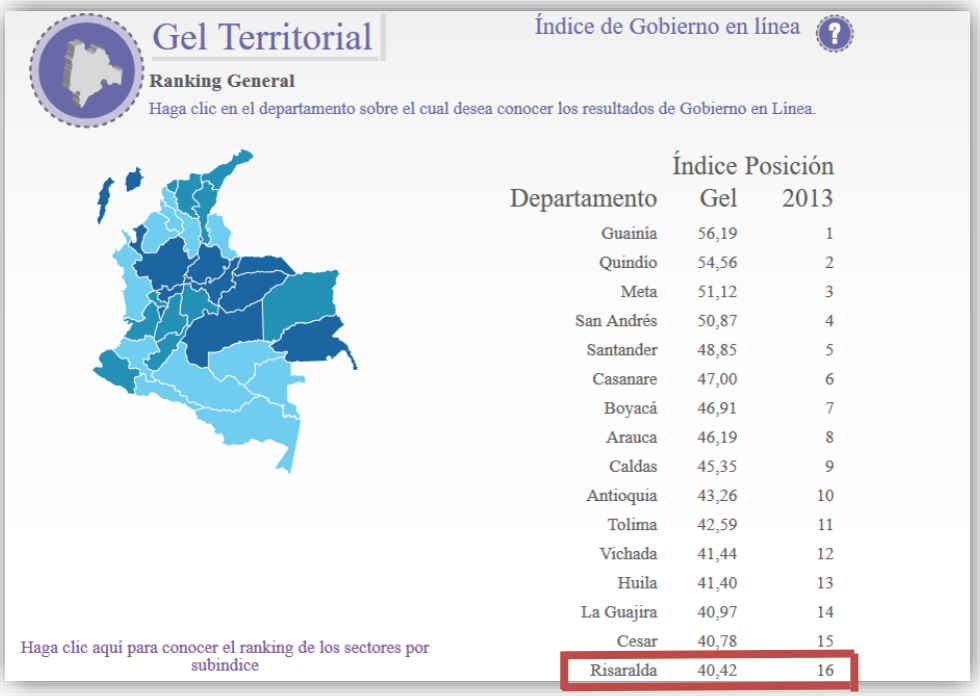
Gráfica 2: Representación de los avances de las entidades en la ejecución de la estrategia GEL de orden Nacional Fuente: Índice de Gobierno en Línea

Al observar el índice GEL en el 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 (Ver gráfica 3 tomado de (GEL, 2015) Recuperado el día

4 de mayo de 2016), lo que ubica el departamento de Risaralda en el puesto número 16 de los 32 departamentos medidos.



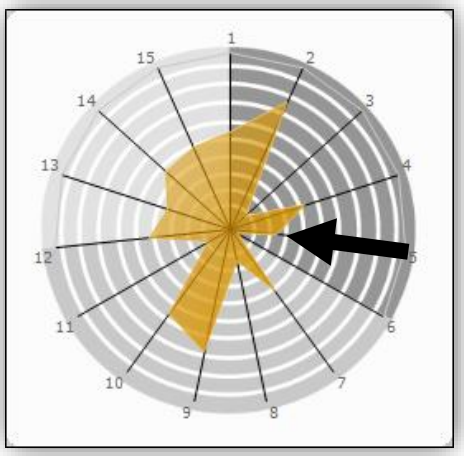
Gráfica 3: Representación de los avances de las entidades en la ejecución de la estrategia GEL de orden Territorial Fuente: Índice de Gobierno en Línea



Departamento	Índice Gel	Posición 2013
Guainía	56,19	1
Quindío	54,56	2
Meta	51,12	3
San Andrés	50,87	4
Santander	48,85	5
Casanare	47,00	6
Boyacá	46,91	7
Arauca	46,19	8
Caldas	45,35	9
Antioquia	43,26	10
Tolima	42,59	11
Vichada	41,44	12
Huila	41,40	13
La Guajira	40,97	14
Cesar	40,78	15
Risaralda	40,42	16

Gráfica 4 Representación de la posición de los Departamentos, frente a la implementación de GEL Fuente: Índice de Gobierno en Línea

El índice interno para el 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.



Gráfica 5: Representación de los avances de las entidades en la ejecución de la estrategia GEL del departamento de Risaralda Fuente: Índice de Gobierno en Línea

Al indagar sobre las entidades estatales que han venido desarrollando actividades relacionadas al Numeral 5 del Subíndice Eficiencia Electrónica se observa que se hace un gran esfuerzo en torno a las administraciones municipales (Alcaldías) y en la gobernación de Risaralda, sobresaliendo la Alcaldía de Dosquebradas y la Alcaldía de Pereira mediante la puesta a disposición de los ciudadanos de portales tributarios y APPs de consulta de vendedores informales, así como la consulta interactiva del plan de desarrollo.

Lo anterior corrobora la necesidad que se tiene de diagnosticar el grado de madurez de los controles de seguridad de la información con el fin de determinar los controles aplicables para las instituciones educativas de nivel preescolar, dado que se constituye en un sector carente del desarrollo de acciones tendientes al cumplimiento de las actividades enunciadas en la Estrategia de Gobierno en Línea (GEL) y el Ministerio de Tecnología de la Información y la Comunicación (MINTIC)

1.4 PLANTEAMIENTO DE HIPÓTESIS

¿Cómo asegurar la confidencialidad, integridad, disponibilidad y control de la información en las instituciones educativas de nivel preescolar de la comuna Universidad de la Ciudad de Pereira, de acuerdo a los controles establecidos por la norma NTC ISO/IEC 27001:2013?

1.5 IDENTIFICACIÓN DE VARIABLES

N/A

1.6 PRESUPUESTO

Tabla 1: Presupuesto del proyecto global Fuente: Propia – 2016

PRESUPUESTO GLOBAL	
RUBROS	**TOTAL**
1. GASTOS DE PERSONAL	$29.120.000
2. GASTOS DE VIAJE	$192.000
3. INVERSIONES	$3.742.000
4. GASTOS GENERALES	$56.200
5. SERVICIOS TÉCNICOS	$60.000
TOTAL	**$33.170.200**

Tabla 2: Presupuesto detalles de gastos personales Fuente: Propia – 2016

1. DETALLE GASTOS DE PERSONAL						
NOMBRE DEL PARTICIPANTE	**NIVEL DE FORMACIÓN**	**ROL EN EL PROYECTO**	**HORAS SEMANALES DEDICADAS AL PROYECTO**	**N° DE MESES**	**VALOR / HORA**	**TOTAL**
LILIANA GRAJALES	TECNOLOGA	INVESTIGADOR	16	7	$20.000	$8.960.000
MONICA LEÓN	TECNOLOGA	INVESTIGADOR	16	7	$20.000	$8.960.000
CARLOS ARTURO BLANDON	MAGISTER	ASESOR	8	7	$50.000	$11.200.000
					TOTAL GASTOS DE PERSONAL	**$29.120.000**

Tabla 3: Presupuesto detalles gastos de viaje Fuente: Propia - 2016

1. DETALLE GASTOS DE VIAJE							
LUGAR DE ORIGEN	LUGAR DE DESTINO	TRAYECTO	N° DE DÍAS	N° DE PERSONAS	VALOR VIATICOS POR PERSONA	JUSTIFICACION	TOTAL
Centro	IE La Julita	Ida y regreso	1	2	$12.000	Primer acercamiento	$24.000
Centro	IE La Julita	Ida y regreso	1	2	$12.000	Levantamiento de información	$24.000
Centro	Remigio Antonio Cañarte	Ida y regreso	1	2	$12.000	Primer acercamiento	$24.000
Centro	Remigio Antonio Cañarte	Ida y regreso	1	2	$12.000	Levantamiento de información	$24.000
Centro	Técnico Superior	Ida y regreso	1	2	$12.000	Primer acercamiento	$24.000
Centro	Técnico Superior	Ida y regreso	1	2	$12.000	Levantamiento de información	$24.000
Centro	Mariela Lemus	Ida y regreso	1	2	$12.000	Primer acercamiento	$24.000
Centro	Mariela Lemus	Ida y regreso	1	2	$12.000	Levantamiento de información	$24.000
TOTAL GASTOS DE VIAJE							**$192.000**

Tabla 4: Presupuesto detalles inversiones Fuente: Propia – 2016

3. DETALLE 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	Imprimir documentación del proyecto	$300.000
Cartuchos	1	$50.000	Tinta para la impresora	$50.000
Mesas	2	$100.000	Adecuación para la realización del proyecto	$200.000
Sillas	2	$80.000	Adecuación para la realización del proyecto	$160.000
Memoria USB	2	$16.000	Copias de seguridad de la documentación del proyecto y cargar los documentos	$32.000
			TOTAL INVERSIONES	**$3.742.000**

Tabla 5: Presupuesto detalles de gastos generales Fuente: Propia - 2016

4. DETALLE GASTOS GENERALES				
DESCRIPCIÓN DEL ARTÍCULO	**CANTIDAD**	**VALOR UNITARIO**	**JUSTIFICACIÓN**	**TOTAL**
Lapiceros	4	$800	Escribir anotaciones	$3.200
Cuadernillo	2	$1.000	Guardar 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
Sacapuntas	4	$400	Sacar punta a los lápices	$1.600
Encuadernación	1	$20.000	Encuadernar el informe Final	$20.000
Resma de papel	2	$10.200	Impresiones	$20.400
			TOTAL GASTOS GENERALES	$56.200

Tabla 6: Presupuesto detalles servicios técnicos Fuente: Propia - 2016

5. DETALLE SERVICIOS TÉCNICOS				
DESCRIPCIÓN DEL SERVICIO TÉCNICO	**CANTIDAD**	**VALOR UNITARIO**	**JUSTIFICACIÓN**	**TOTAL**
Internet	1	$ 60.000	Consultas	$60.000
			TOTAL SERVICIOS TÉCNICOS	$60.000

1.7 CRONOGRAMA

Tabla 7: Descripción detallada de las actividades a realizar durante el proyecto.

MES	OCTUBRE				NOVIEMBRE				FEBRERO				MARZO				ABRIL				MAYO			
ACTIVIDAD	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Estudio del marco legal del Ministerio de Educación Nacional																								
Estudio del marco legal de Gobierno en Linea																								
Estudio de los controles de seguridad de la información de la Norma NTC/ISO IEC 27001:2013																								
Generación de catálogo de activos																								
Análisis de la criticidad de los activos de información																								
Identificación de los escenarios de riesgos																								
Realización de las pruebas de penetración																								
Calificación de los riesgos inherentes creación de los mapas de temperatura de los riesgos inherentes																								
Identificación de los controles aplicables a los excenarios de riesgo identificados																								
Calificación de los riesgos residuales																								
Mapas de temperaturas de los riesgos residuales																								
Plan de mitigación del riesgo																								
Propuesta de la declaración de aplicabilidad																								
Identificación de los controles aplicables de acuerdo al análisis de riesgos																								
Entrega de informe final.																								

2. MARCO CONTEXTUAL.

2.1 EL ENTORNO ESCOLAR

En la declaración universal de los derechos humanos se encuentra el derecho a la educación, sobre el particular el Movimiento de los Pueblos para la Educación de los Derechos Humanos a través de su sitio web http://www.pdhre.org/ define el derecho humano a la educación de la siguiente manera:

> “Cada mujer, hombre, joven y niño o niña tienen el derecho a la educación, capacitación e información; así como a otros derechos humanos fundamentales para la realización plena de su derecho a la educación. El derecho de todas las personas a la educación se encuentra establecido en la Declaración Universal de los Derechos Humanos, Pactos Internacionales, la Convención de los Derechos del Niño y otros tratados y declaraciones internacionales; “todas éstas forman parte de herramientas poderosas que deben ser puestas en marcha para el goce del derecho a la educación para todos." (Koenig, 2016)

En coherencia con la Declaración Universal de los Derechos Humanos, la República de Colombia reglamenta la educación desde los derechos fundamentales que se incluyen en la Constitución Política, en virtud de lo cual para contextualizar la problemática estudiada de manera adecuada es necesario abordar el marco jurídico de los entornos escolares presentes en Colombia y la relación que se genera entre dicho marco y los requerimientos de seguridad de la información emanados por el Ministerio de Tecnologías de Información y Comunicación, la Estrategia de Gobierno en Línea y los requisitos de la Norma ISO/IEC 27001.

Se parte entonces desde el artículo 44 de la Constitución Política de Colombia de 1991, que menciona como derecho fundamental de los niños el derecho a la educación:

> “Artículo 44. 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.
>
> La familia, la sociedad y el Estado tienen la obligación de asistir y proteger al niño para garantizar su desarrollo armónico e integral y el ejercicio pleno de sus derechos. Cualquier persona puede exigir de la autoridad competente su cumplimiento y la sanción de los infractores. Los derechos de los niños prevalecen sobre los derechos de los demás." Art. 44, (Constitución Política de Colombia, 1991, pág. 24)

Lo que es consagrado como derecho fundamental constitucional mediante el artículo 67 de la misma constitución, el cual en uno de sus apartados reza "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)

De manera congruente con lo exigido actualmente por el Ministerio de Tecnologías de la Información y la Comunicación - MINTIC, la Estrategia de Gobierno en Línea y los principios de la Norma Internacional ISO/IEC 27001 este mismo artículo 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." , Art. 67, (Constitución Política de Colombia, 1991, pág. 36) lo cual muestra que desde la constitución se ha establecido la finalidad de velar por la calidad así como el adecuado cubrimiento del servicio, implicando la confiabilidad, disponibilidad e integridad que persigue la actividad 4 de los lineamientos de la Estrategia de Gobierno en Línea y que han sido referenciados en los manuales técnicos emitidos por el Ministerio de Tecnologías de Información y Comunicación – MINTIC en relación al establecimiento de un Sistema de Gestión de Seguridad de la Información – SGSI.

No obstante, 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:

> "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)

Dando claridad al alcance de los niveles educativos respecto al Artículo 11 de la Ley General de Educación, se establece que la educación formal se organizará en tres (3) niveles:

> 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)

De igual manera se define la educación preescolar como: "La educación preescolar corresponde a la ofrecida al niño para su desarrollo integral en los aspectos biológico, cognoscitivo, sicomotriz, socio-afectivo y espiritual, a través de experiencias de socialización pedagógicas y recreativas". Art. 15, (Ley 115, 1994, pág. 5)

Lo que define de manera clara que el nivel preescolar esta categorizado como nivel de formación desde la jurisprudencia nacional. La misma Ley General de Educación en su artículo 2 establece que el servicio educativo está comprendido por

> "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 cual se traduce en que el servicio educativo de nivel preescolar tiene dentro de sus elementos constitutivos aquellos relacionados a las normas jurídicas que rigen a las entidades de carácter oficial, así como los recursos tecnológicos que soportan

la operación de la Institución Educativa, evidenciando de igual manera la concepción de una administración basada en procesos permitiendo una aproximación a la norma ISO/IEC 27001 la cual está basada igualmente en procesos, tal como puede verse en el numeral 0,1 de la misma.

Es importante definir desde el punto de vista histórico cómo se gestó el nivel educativo preescolar y cómo lo define la legislación colombiana, de tal manera que se resalte la importancia de un servicio de calidad, fundamental en esta etapa temprana y de gran importancia para el desarrollo de los niños y para la sociedad en general, al igual que permita crear un contexto a modo de marco de referencia.

Necesario es entonces notar que la educación preescolar en Colombia ha evolucionado con el pasar del tiempo. Inicialmente era de carácter asistencial, concentrando la atención a los niños y niñas de menos de 7 años en asilos cuyo propósito era su cuidado y protección. Con el pasar del tiempo, estos asilos atendían particularmente a la niñez abandonada, siendo en su gran mayoría menores de 6 años, factor que desencadenó en la necesidad de proponer actividades lúdicas y educativas, sin que este constituyera el objetivo de los asilos.

Hacia 1930, algunos de estos centros estaban orientados por religiosas, señalando el primer antecedente de educación preescolar, valorando el carácter educativo de la actividad, aunque no estuviera reconocida legalmente, situación que continuo hasta mediados de 1975.

El servicio educativo a este nivel solo se ofrecía a familias que tuvieran buena posición económica, situación que cambio cuando el papel de la mujer como participante activa del mundo laboral, permite la generación de una alternativa para la población de escasos recursos económicos, que en su inicio estuvo apalancado por el Instituto Colombiano de Bienestar Familiar ICBF, pero éste se sujetó a las normas de protección del menor desde el punto de vista asistencial y dejo de lado la parte educativa.

En 1976, mediante el Decreto 088 del Ministerio de Educación Nacional – MEN se da reconocimiento por primera vez a la educación preescolar dentro del sistema educativo colombiano, el cual tenía por objetivos la promoción y estimulación de desarrollo físico, afectivo y espiritual del niño, su integración social, su percepción sensible y el alistamiento para la etapa escolar. En este mismo año se reconoce por primera vez el estatus de Carrera Profesional a la educación preescolar, lo que se convirtió en el punto de partida para la regulación y organización de la actividad educativa y pedagógica de los establecimientos de educación preescolar.

En 1987 se precisaron las áreas y temas relacionados con el preescolar, permitiendo la generación de currículos fundamentados desde lo teórico al igual que la regulación de la operatividad de las instituciones que tenían este nivel de educación.

De esta manera en 2001, mediante la ley 715 del 21 de diciembre se define institución educativa en el artículo 9 de la siguiente manera:

> "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)

Con lo que podemos observar la obligatoriedad de un año para la educación preescolar y su inclusión como institución de educativa reconocida legalmente, por lo tanto, se especifican las competencias frente a los municipios las cuales constituyen: "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)

Lo que implica que las actividades administrativas de dirección y planificación para la adecuada prestación del servicio, enmarcando estás en un mundo globalizado, dinámico desde el punto de vista de la competitividad generada a través de la inclusión de tecnologías de información, que fortalecen la operatividad pero que a la vez generan nuevos riesgos de seguridad para el tratamiento de información; tengan presente la adopción, mantenimiento y cuidado de un sistema de información para este sector educativo conforme lo dispone la Ley 715 en el artículo 5, numeral 5.4.

La misma Ley indica que una de las competencias de los distritos y los municipios certificados es la de "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

> "...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)

Los sistemas de información que permitan facilitar la prestación del servicio por parte de la institución educativa deberán mantenerse actualizados de acuerdo con las orientaciones que para tal fin determine la nación, lo que vislumbra aún más la articulación que existe entre la Estrategia de Gobierno en Línea y los mandatos legales para las entidades que prestan servicios educativos de nivel preescolar.

2.2 MARCO LEGAL DEL ENTORNO ESCOLAR RELACIONADO CON LA SEGURIDAD DE LA INFORMACIÓN

Debido al gran avance tecnológico y la contribución a mejorar los procesos en cuanto a transparencia y eficiencia en la gestión estatal, el gobierno nacional ha decretado y generado las directrices necesarias para la incorporación de las TIC en todos los procesos, trayendo consigo una evolución permanente en su implementación en cada una de las entidades del país, pues las TIC se han convertido en una herramienta fundamental, mejorando los procesos de gestión entre las entidades del estado y los ciudadanos, es por ello que la Estrategia de Gobierno en Línea (GEL), es considerada un eje fundamental.

Gobierno en línea en Colombia inició en el año 2000, pero continuo de forma decidida desde el año 2008 con el decreto 1151 que definió los lineamientos generales de la Estrategia de Gobierno en Línea.

La implementación de las TIC ha generado beneficios importantes como agilidad en los trámites y servicios a través de medios electrónicos, mejora en la calidad de la información en sitios web logrando ofrecer a todos los ciudadanos el 100% de la

información a través de plataformas virtuales, además de espacios para la participación ciudadana.

Siendo coherentes con la naturaleza de las Instituciones Educativas Públicas del orden territorial, se hace necesario acatar lo descrito en el Decreto 1078 del 26 de mayo de 2015**,** donde se describen las directrices que todas las instituciones de carácter público deben seguir con el objetivo de acogerse a la Estrategia de Gobierno en Línea - GEL, implicando obligatoriedad para las instituciones educativas de carácter oficial que tienen dentro de sus niveles educativos el preescolar.

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 que 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) de tal manera que se garantice el máximo aprovechamiento de las Tecnologías de Información y comunicación.

La aplicación del título 9 del Decreto 1078 cobija todas “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 Gobierno en Línea 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)

Se definen de esta manera los 4 componentes que facilitarán la oferta y la demanda de la Estrategia de Gobierno en Línea:

1. TIC para Servicios. Comprende la provisión de trámites y servicios a través de medios electrónicos, enfocados a dar solución a las principales

necesidades y demandas de los ciudadanos y empresas, en condiciones de calidad, facilidad de uso y mejoramiento continuo.

2. TIC para el Gobierno abierto. Comprende las actividades encaminadas a fomentar la construcción de un Estado más transparente, participativo y colaborativo involucrando a los diferentes actores en los asuntos públicos mediante el uso de las Tecnologías de la Información y las Comunicaciones.

3. TIC para la Gestión. Comprende la planeación y gestión tecnológica, la mejora de procesos internos y el intercambio de información. Igualmente, la gestión y aprovechamiento de la información para el análisis, toma de decisiones y el mejoramiento permanente, con un enfoque integral para una respuesta articulada de gobierno y para hacer más eficaz la gestión administrativa entre instituciones de Gobierno.

4. Seguridad y privacidad de la Información**.** Comprende las acciones transversales a los demás componentes enunciados, tendientes a proteger la información y los sistemas de información, del acceso, uso, divulgación, interrupción o destrucción no autorizada. Titulo 9, Capítulo 1, Sección II, Art, 2.2.9.1.2.1 (Decreto 1078, 2015, pág. 136)

Se pone en manifiesto entonces el hecho de proteger la información y los sistemas de información de todos los menores de preescolar que se matriculan en instituciones educativas oficiales, lo cual se puede conseguir mediante un adecuado mapeo de los riesgos inherentes a la prestación del servicio educativo y por consiguiente la adopción de acciones tendientes a mitigar los mismos.

El Gobierno Nacional ha puesto a disposición de las entidades estatales que pretendan dar cumplimiento a los dispuesto en GEL 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), de igual manera ha dispuesto un instrumento que permite realizar el diagnóstico inicial de la entidad que desea iniciar el proceso de implementación del Sistema de Gestión de Seguridad de la Información, constituyéndose este en un punto de partida para la toma de decisiones con respecto de las actividades requeridas para cerrar las brechas existentes entre lo que exige GEL y lo que la entidad actualmente tiene.

Es importante resaltar que la Ley 1581 del 17 de octubre de 2012, mediante la cual se dictan las disposiciones generales para la protección de los datos personales establece en el artículo 7 que:

> " 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)

Se pone en evidencia entonces la importancia que para el gobierno nacional tiene la protección de la información de los niños y niñas, al igual que la transparencia y la comunicación con la ciudadanía que persigue a través de la implementación de la Estrategia de Gobierno en Línea, específicamente desde su actividad 4, confluyendo entonces la Constitución Política, el Ministerio de Educación, el Ministerio de Tecnologías de la Información y la Comunicación con lo dispuesto por la norma internacional ISO/IEC 27001 que describe cómo gestionar la seguridad de la información, y que es referente para las herramientas que sobre el tema tiene el MINTIC.

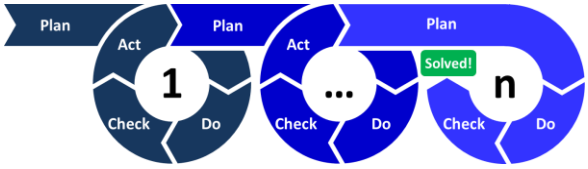
2.3 IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN EN EL ENTORNO ESCOLAR

Determinar el grado de madurez de los controles basado en la Norma Internacional ISO/IEC 27001 en las instituciones públicas de educación Preescolar genera los siguientes beneficios:

1. Disposición de una metodología de administración de riesgos: a través de la cual será posible identificar, categorizar y priorizar los riesgos del entorno escolar relacionados con la seguridad de la información, estableciendo controles que permitan la mitigación de los mismos, generando confianza en todos los usuarios del servicio educativo.

2. Mejora continua en la gestión de la seguridad: La Norma Internacional ISO/IEC 27001 basa su funcionamiento en la metodología del circulo de Deming (P – Planear, H – Hacer, V – Verificar, A - Actuar) lo que implica el impetuoso requerimiento de realizar auditorías internas que impulsan

permanentemente a la adopción de acciones preventivas y correctivas que permiten la identificación de nuevos riesgos y la ratificación de que los controles adoptados han dado los resultados deseados.



Gráfica 6: Múltiples iteraciones circulo de Deming. Fuente: Christoph Roser at AllAboutLean.com

3. Disponibilidad del Servicio Educativo: Poseer un mapa de riesgos definido, y más aún los controles asociados a cada uno de los mismos lo que conlleva a aproximarse cada vez más a la “No Parálisis” del servicio educativo ocasionada por temas relacionados a la seguridad de la información, garantizando la continuidad de la atención en términos de oportunidad.

4. Reducción de costos de incidentes e inversiones: Con una filosofía basada en el tratamiento de riesgos, la Norma Internacional ISO/IEC 27001 permite anticiparse a los posibles desastres y parálisis de operatividad de los procesos organizacionales que se traducen en incidentes que deterioran y ponen en riesgo la seguridad de la información, evitando sobrecostos ocasionados por daños, reprocesos o demandas generadas por el no tratamiento oportuno de los riesgos.

5. Cumplimiento de la legislación: Es una apuesta a cerrar las brechas de cumplimiento normativo 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.

6. Incremento de los niveles de confianza de las partes interesadas

7. Mejora imagen institucional

8. Formalización de responsabilidades operativas: dado que la Norma Internacional ISO/IEC 27001 está basada en procesos, permite definir y describir de manera detallada y formal las actividades tendientes a la seguridad de la información en cada uno de los eslabones que conforman la institución educativa y que son vitales para el tratamiento de información en los diferentes estadios por los cuales esta pasa.

Todos estos aspectos se traducen en los tres pilares emanados de la norma y perseguidos por la estrategia de GEL disponibilidad, integridad y seguridad de la información.

2.4 DIRECTRICES Y LINEAMIENTOS DEL MINISTERIO DE EDUCACIÓN NACIONAL

El Decreto 1075 del 26 de mayo de 2015, indica que: "Los municipios con más de 100.000 habitantes deben cumplir con los siguientes requisitos:

a) Plan de desarrollo municipal, armónico con las políticas educativas nacionales;

b) Establecimientos educativos estatales organizados para ofrecer, por lo menos, el ciclo de educación básica completa;

c) Planta de personal docente y directivo docente definida de acuerdo con los parámetros nacionales;

d) Capacidad institucional para asumir los procesos y operar el sistema de información del sector educativo." Art, 2.3.1.1.2 (Decreto 1075, 2015, pág. 11)

Lo que muestra que desde la concepción normativa del Ministerio se adoptan directrices que generan congruencia con GEL desde la capacidad con la cual se administran los sistemas de información mediante los cuales los establecimientos educativos prestan el servicio educativo.

“La prestación del servicio público educativo del nivel preescolar se ofrecerá a los educando de 3 a 5 años de edad”, comprendiendo pre – jardín, jardín y transición, Art, 2.3.3.2.2.1.2 (Decreto 1075, 2015, pág. 89) dado tal servicio “con base en los lineamientos del MEN, ejecutado con un plan que permita asumir procesos de calidad” Art, 2.3.1.1.6 (Decreto 1075, 2015, pág. 12)

Estos procesos de calidad se deben enmarcar dentro de las características de disponibilidad, seguridad y confiabilidad que se pueden soportar desde el adecuado manejo de los sistemas de información.

2.5 ESTRUCTURA DE UN ESTABLECIMIENTO EDUCATIVO

Los establecimientos educativos tienen estructuras diferentes de acuerdo con su tamaño, si bien las directrices del MEN no establecen una estructura organizacional particular, se puede generalizar de la siguiente manera:

1. Rector
2. Secretaria Rectoría
3. Tesorero
4. Secretaria Académica
5. Psicólogo
6. Coordinadores
7. Docentes
8. Personal de apoyo (Personal de aseo, jardineros, seguridad)

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.

Sin embargo, no se define una estructura única para estas instituciones y se organiza de conformidad a la necesidad del propio establecimiento y la cobertura en términos de personas atendidas en cada claustro educativo.

3. MARCO TEÓRICO

3.1 INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN

Se entiende por información al conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o se transmita, de su origen o de la fecha de elaboración.

Se llama seguridad de la información al conjunto de políticas, estándares y controles que se implementan en una organización para preservar la confidencialidad, la integridad y la disponibilidad de la información, además de las características fundamentales mencionadas se debe tener en cuenta:

a. Autenticación: Provisión de una garantía de que una característica afirmada por una entidad es correcta. (NTC ISO/IEC 27001, 2013) Permite identificar a la persona o personas que han generado la información que se está verificando.

b. No repudio: Servicio que permite probar la participación de las partes en una comunicación. (Calvo García, 2014) También definido como el servicio de seguridad que previene que un emisor niegue haber remitido un mensaje y que un receptor niegue su recepción. (OSI ISO-7498-2, 1989)

Las anteriores y los controles establecidos en la norma son propiedades mínimas que debe tener un SGSI, para asegurar la confidencialidad, integridad y seguridad de la información de la organización.

3.1.1 Activo de información

Se define activo como cualquier cosa que tenga un valor para la organización, sean estos de carácter tangible o intangible. Por cuanto es necesario identificar aquellos activos que son críticos para el adecuado funcionamiento de los procesos en la institución educativa, y que son fundamentales para el diagnóstico del grado de madurez de los controles de seguridad de la información.

Contextualizando el anterior concepto al sector educativo de las entidades oficiales de nivel preescolar se han considerado como activos los siguientes:

a. Información de los educandos
b. Servicios y equipos de tecnologías de información.
c. Hardware y software
d. Servicios y equipos de comunicación

3.1.2 Riesgo

Definido por la Real Academia de la lengua como “proximidad o contingencia de un posible daño”, por la Norma Internacional ISO/IEC 31000 como “Efecto de la incertidumbre sobre los objetivos” (ISO/IEC 31000, 2009), por el Marco de Gestión de riesgos COSO como “La probabilidad que ocurra un determinado evento que puede tener efectos negativos para la institución” (Condori Benavides, 2015, pág. 3), y por ISACA, COBIT como “Un riesgo para el negocio, específicamente el riesgo para el negocio asociado con el uso, propiedad, operación, involucramiento, influencia y adopción de TI en una empresa”. (ISACA, 2013) Se entiende entonces el riesgo como la probabilidad de ocurrencia de un daño a la información administrada con o sin intervención de un sistema de información.

Ampliando entonces la definición de riesgo podría considerarse como la combinación de la probabilidad de que ocurra un incidente con el impacto generado en los procesos involucrados en el caso de que este ocurriera.

Cuando existen probabilidades de que los riesgos se materialicen, se crea incertidumbre, produciendo una necesidad imperiosa de realizar análisis de riesgos, para lo cual se deben tener en cuenta las siguientes características:

a. Evento o incidente: suceso futuro del que no se tiene certeza de ocurrencia, y están asociado con consecuencias en los procesos donde se presenta.

b. Activo: Algo que representa un valor para la institución educativa, que se ve afectado con la ocurrencia de un incidente.

c. Consecuencia o daño: Impacto que tiene la ocurrencia del incidente sobre el activo, presupone un daño total o parcial del activo relacionado.

d. Probabilidad: medición de la posibilidad de ocurrencia del riesgo identificado, generando un valor que permite realizar el proceso de priorización y catálogo de los mismos, permitiendo crear una base esencial para el establecimiento de los controles para su mitigación.

e. Impacto: medición de la afectación sobre el activo que produciría la ocurrencia del incidente, permite realizar el proceso de priorización y catálogo del riesgo.

La incertidumbre generada por los riesgos identificados, requiere que se protejan los activos de los procesos organizacionales, mediante un adecuado tratamiento de riesgos, el cual puede abarcarse mediante las siguientes fases:

a. Identificación y valoración de activos: abarca el estudio de las actividades de la institución educativa, dicho estudio consiste en el uso de técnicas y herramientas metodológicas tales como entrevistas, encuestas, documentación existente, observación, registro fotográfico, entre otros.

b. Identificación y valoración de riesgos: se realiza un análisis de riesgos y amenazas existentes, estableciendo la probabilidad de ocurrencia y el impacto generado por su materialización. Lo cual permitirá realizar la priorización de los riesgos en función de la [Probabilidad X Impacto], de acuerdo a los resultados obtenidos se decide aceptar o no los riesgos en función de las tablas que para tal efecto que se hayan diseñado durante el análisis.

c. Implementación de controles: Se establecen los controles que permiten la mitigación del impacto o la probabilidad de ocurrencia del riesgo.

3.2 SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Nace como respuesta a la necesidad de protección de la información del sector empresarial, también es nombrado como SGSI o ISMS – Information Security Management System. Pretende controlar el acceso de personas no autorizadas y las consecuencias generadas por la ocurrencia de los riesgos inherentes a los cuales se encuentra expuesta la información de los diferentes procesos de la organización, permitiendo la formulación de acciones que procuren la continuidad de las operaciones.

Contiene el catálogo de los activos de información que deben protegerse, dada la importancia que tienen para la operatividad de los procesos organizacionales, los riesgos y amenazas a lo que están expuestos y los controles adoptados para mitigar y preservar los activos.

Como fundamentos para garantizar que la seguridad de la información es gestionada correctamente se debe identificar inicialmente su ciclo de vida y los aspectos relevantes para garantizar la confidencialidad, integridad y disponibilidad. Conocido el ciclo de vida de la información, es necesario adoptar un proceso sistemático, documentado y conocido por la organización con enfoque a la gestión del riesgo.

Lo anterior con el propósito de garantizar que los riesgos son conocidos, asumidos, gestionados y mitigados de forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. (ISO 27000.ES, 2005) Recuperado el día 5 de enero de 2016

Gráfica 7: Circulo de riesgos Fuente: http://www.iso27000.es/sgsi.html

3.3 DIFERENCIAS ENTRE SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD INFORMÁTICA.

La información hoy por hoy evoca un sin número de temores tanto para las personas naturales como para las personas jurídicas, en razón a que contemplar y mantener la información bajo control sin fugas y sin intrusiones ha sido un gran reto, llevando a que la información se considere como uno de los activos más importantes, para la cual las Tecnologías de Información y Comunicación han sido, son y serán el mecanismo más idóneo para su manipulación tanto en equipos de escritorio como en la nueva ola de almacenamiento cloud y la incursión del BigData.

Los procesos relativos al procesamiento, almacenamiento y distribución de la información han cambiado su forma de operación con la incursión de las Tecnologías de Información y Comunicación TIC, permitiendo el acceso desde cualquier punto y casi en cualquier momento, pero de la misma manera generando vulnerabilidades que avocan a la seguridad de la información y de los medios que se utilizan para su tratamiento.

Eventos de amplia difusión pública de incidentes como la divulgación de correos diplomáticos de las embajadas americanas (difundidos por la red Wikileaks), la sustracción de información de más de 75.000 usuarios de los servicios de juegos en línea de la multinacional SONY y el ataque a los sitios web estatales en Colombia (por parte del grupo Anonymus a raíz de la promoción de la llamada Ley lleras) o a sitios del gobierno de los Estados Unidos por el anuncio de las leyes SOPS y PIPA; son solo una pequeña muestra del incremento vertiginoso de las amenazas a la seguridad de la información, amenazas que han llevado a las empresas a preocuparse por los niveles de protección de sus activos de información y a preguntarse si estos están correctamente identificados y valorados. (Caviedes Sanabria & Prado Urrego, 2012) (Tesis de Maestría). Universidad ICESI, Santiago de Cali, Colombia

Teniendo presente la exigencia realizada a las entidades del estado desde la estrategia de Gobierno en Línea sobre la implementación de un Sistema de Gestión de Seguridad de la Información, se hace necesario aclarar la diferencia que existe entre seguridad de la información y seguridad informática para todas las partes interesadas, de tal manera que queden en manifiesto las diferencias e implicaciones de cada una de ellas.

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. (NTC ISO/IEC 27001, 2013)

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)

Es un hecho entonces que la seguridad informática y la seguridad de la información se encuentran relacionadas desde la confianza y control que se debe tener para cumplir con las características indicadas por ISO/IEC 27001 de integridad, confiabilidad y disponibilidad.

3.4 CRITERIOS DE SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información está enmarcada bajo tres criterios, promovidos por la ISO/IEC 27001 y adoptados por la estrategia de Gobierno de Línea – GEL

a. Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. (ISO/IEC 27000, 2014, pág. 8)

b. Integridad: Propiedad de la información relativa a su exactitud y completitud. Implica la protección de la información contra modificación o eliminación sin autorización. (ISO/IEC 27000, 2014, pág. 11)

c. Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera la entidad. (ISO/IEC 27000, 2014, pág. 8)

Gráfica 8: Pilares de la seguridad de la información fuente propia

La información, en conjunción con los procesos y los sistemas que hacen uso de ella, son activos importantes, por cuanto las características anteriormente mencionadas pueden ser esenciales para la competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para alcanzar las metas de la organización.

3.5 FAMILIA DE NORMAS ISO/IEC 27000

Desde 1901, la British Standar Institution BSI, se constituyó como la primera entidad de normalización a nivel mundial, publicando entre otras: la BS 5750 ahora ISO 9001, la BS 7750 ahora ISO 14001 y la BS 8800 ahora OHSAS 18001.

La BS 7799 aparece en 1995, proporcionando un conjunto de buenas prácticas para la gestión de la seguridad de la información, compuesta por dos partes la BS 7799-1 que es la guía de buenas prácticas y la BS 7799-2 que establece los requisitos de un sistema de seguridad de la información.

La organización Internacional de Estandarización, es la encargada de difundir los estándares de aceptación mundial en temas relacionados con el ambiente, la salud, las tecnologías, la gestión de calidad, etc. Teniendo en cuenta el crecimiento desmesurado de los índices de incursión de las tecnologías de información y comunicación a nivel de hardware y software en los diferentes niveles organizacionales en todos los sectores industriales, la ISO ha publicado diversos estándares que regulan el ciclo de vida del software, sistemas de información y seguridad de la información.

Es así como la BS 7799-1 se revisó en 1999 y se adoptó por la ISO en el año 2000 como ISO 17799.

En 2002, se revisó BS 7799-2 adecuándose a la filosofía de normas ISO de sistemas de gestión.

En 2005, se publicó el estándar ISO 27001 y se renombro la ISO 17799 como ISO 27002

La familia ISO 27000, es realmente una serie estándares con numeración que va de 27000 a 27019 y de 27030 a 2044.

Con respecto a la seguridad de la información, la ISO publicó la familia de normas de la serie 27000, enfocadas a la estandarización de aspectos relacionados con la gestión de seguridad de la información.

Relación de las principales normas de la serie:

a. ISO 27000, Information Technology – security techniques – information security management systems – overview and vocabulary. Contiene términos y definiciones que se emplean en toda la serie 27000.

b. ISO 27001, Information security management systems – requirements. Especificación de los requisitos del sistema de gestión de seguridad de la información.

c. ISO 27002, Code of practice for information security controls. Guía de recomendaciones y buenas prácticas en gestión de seguridad de la información.

d. ISO 27003, Information security management system implementation guidance. Guía para la implementación de las normas de la serie 27000.

e. ISO 27004, Measurement. Establece las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles asociados.

f. ISO 27005, Informacion security risk management. Presenta una metodología para el análisis de riesgos.

g. ISO 27006, Requirements for bodies providing audit and certification of information security managements systems. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

h. ISO 27007, guidelines for information security management systems auditing. Guía de auditoría para SGSI.

i. ISO 27008 TR, guidelines for auditors on information security controls. Guía para la revisión de la implementación y operación de controles.

j. ISO 27009, Security techniques. Técnicas de seguridad.

k. ISO 27010, Information security management for inter – sector and inter – organisational communications. Gestión de seguridad de la información para las comunicaciones inter – sectoriales e inter – organizacionales.

l. ISO 27011, Information security management guidelines for telecomunications organizations based on ISO/IEC 27002. Guía de seguridad de la información específica para telecomunicaciones.

m. ISO 27014, Governance of information security. Gobernanza de seguridad de la información.

n. ISO 27031, guidelines for information and communications technology readiness for business continuity. Guías de continuidad del negocio en cuanto a tecnologías de la información y comunicaciones.

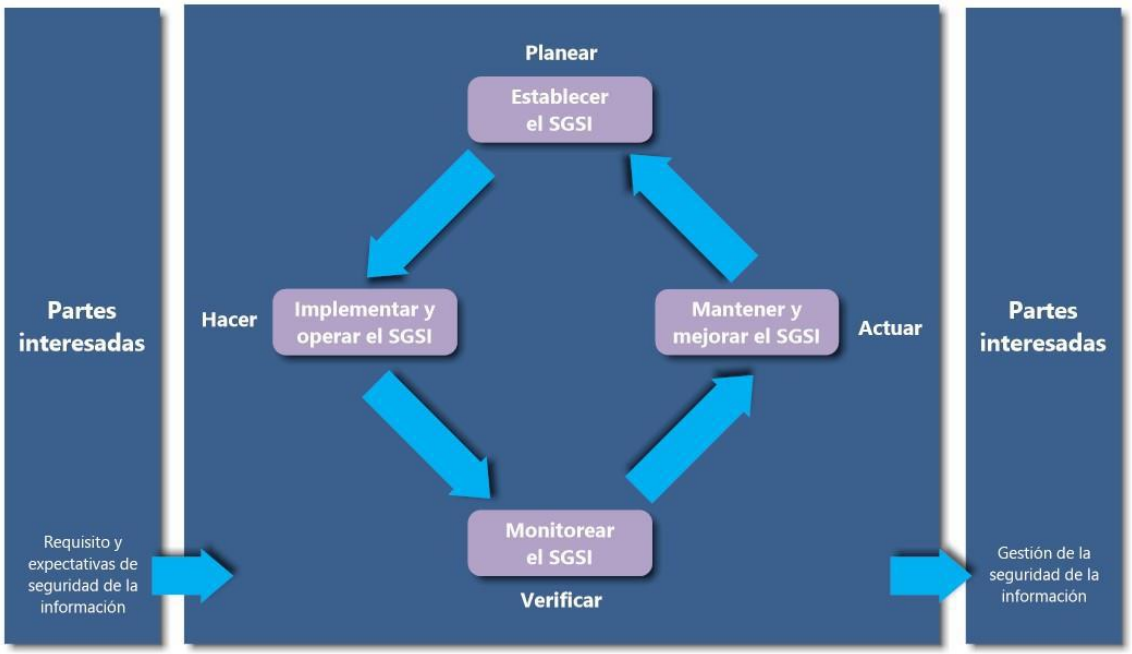
o. ISO 27032, guidelines for cybersecurity. Guía relativa a la ciberseguridad.

3.6 PRINCIPALES NORMAS A UTILIZAR

3.6.1 Norma ISO/IEC 27001

Esta Norma Internacional contiene los requisitos que permiten “el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información”. (NTC ISO/IEC 27001, 2013, pág. 7) Esta Norma tiene un enfoque orientado a procesos, por lo que su campo de aplicación abarca “todas las organizaciones, independientes de su tipo, tamaño o naturaleza”, (NTC ISO/IEC 27001, 2013, pág. 8) permitiendo su adaptación a las instituciones educativas de carácter oficial y nivel preescolar de la comuna universidad de la ciudad de Pereira. Las características actuales de la Norma hacen que sea compatible con otros sistemas de gestión tal como ISO 9001, NTCGP 1000 facilitando su implementación y mantenimiento.

Se constituye entonces en un referente crítico para diagnosticar el grado de madurez de los controles en las instituciones educativas de nivel preescolar de carácter oficial, si bien esta Norma no incluye referencia a la metodología de Deming para la mejora continua, permitiendo la adopción de otros modelos para conseguir tal objetivo, el presente trabajo emplea la metodología de Deming (Plan, Do, Check, Act) como parte integral para diagnosticar el grado de madurez de los controles de seguridad establecidos en la norma



Gráfica 9: Circulo de Deming aplicado al SGSI, basado en NTC ISO/IEC 27001.

3.6.2 Norma ISO/IEC 27001

La Norma Internacional ISO/IEC 27001 contiene una lista de controles para la gestión de la seguridad de la información, por lo tanto, será quien de origen a la declaración de aplicabilidad.

Dicha declaración contendrá los controles que ya se deben implementar y los que son excluidos para las instituciones educativas de educación preescolar.

3.6.3 Norma ISO/IEC 31000

Todos los procesos organizacionales están constantemente sometidos a amenazas desde su contexto interno y externo, generando vulnerabilidades que comprometen la estabilidad de la prestación de sus servicios. Tradicionalmente, los riesgos eran tratados desde la reactividad, pero dada la naturaleza cambiante de los riesgos se ha adoptado una gestión integral de riesgos, que ha permitido el nacimiento de modelos de gestión de riesgos tales como COSO, AS/NZS 4630 e ISO 31000.

La Norma Internacional ISO/IEC 31000 contiene las recomendaciones generales para la gestión del riesgo, y define el riesgo como “El efecto de incertidumbre en la consecución de los objetivos”, (ISO/IEC 31000, 2009, pág. 4) teniendo como manifiesto que este puede ser positivo o negativo y puede que nunca ocurra.

ISO 31000 se basa en once principios:

a. La gestión de riesgos crea valor: apoya el cumplimiento de metas y la mejora del rendimiento operativo de los procesos, así, como “la eficiencia en las operaciones, la gobernanza y la reputación”. (ISO/IEC 31000, 2009, pág. 13)

b. La gestión de riesgos está integrada en los procesos de una organización: se incluye la gestión del riesgo dentro de la planeación estratégica.

c. La gestión del riesgo es parte de la toma de decisiones: permite que los responsables de la toma de decisiones en la organización prioricen las acciones que deben tomarse.

d. La gestión de riesgos trata explícitamente la incertidumbre

e. La gestión del riesgo es sistemática, estructurada y adecuada: buscando resultados comparables, confiables y consistentes.

f. La gestión del riesgo se basa en la mejor información disponible: “se tienen en cuenta la información histórica, experiencia, las partes interesadas observaciones y las opiniones de los expertos”. (ISO/IEC 31000, 2009, pág. 14)

g. La gestión del riesgo está hecha a la medida: alineada con las necesidades del contexto organizacional (Interno y externo).

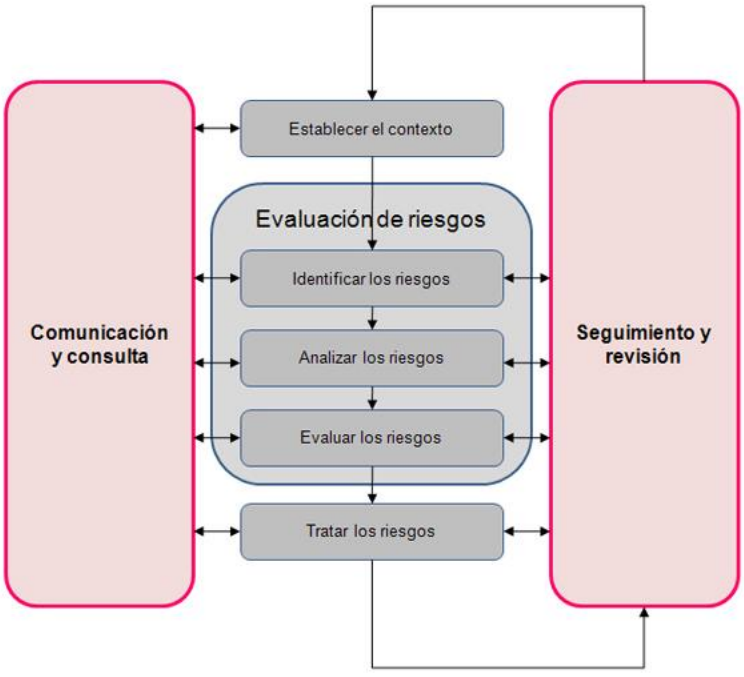
h. La gestión de los riesgos toma en cuenta los factores humanos y culturales: verificando y reconociendo las capacidades, percepciones e intenciones de todas las partes interesadas.

i. La gestión del riesgo es transparente e inclusiva: permitiendo una representación de todas las partes interesadas a fin de que sus percepciones y opiniones sean tenidas en cuenta para determinar los riesgos.

j. La gestión del riesgo es dinámica, interactiva y sensible al cambio: preparando la organización para los cambios de las dinámicas de los contextos internos y externos de tal manera que se encuentre preparada para nuevos riesgos que surjan de dichos cambios.

k. La gestión del riesgo facilita la mejora continua de la organización

En el contexto escolar de las entidades oficiales, y en virtud a los mandatos de la legislación colombiana (MEN, MINTIC), en cuanto al adecuado tratamiento de la información y la adopción de un Sistema de Gestión de Seguridad de la Información propuesto por la actividad 4 de la Estrategia de Gobierno en Línea basado en la norma ISO 27001, que aparte de tener enfoque en procesos, también tiene enfoque en riesgos, es importante la revisión del proceso de gestión de riesgo propuesto por la Norma Internacional ISO/IEC 31000 en la cláusula 6.



Gráfica 10:Proceso De Gestión Del Riesgo. Fuente: http://www.avantium.es/index.php/gestion-de-riesgos-iso-31000

Un adecuado modelo de gestión de riesgos permite entre otros:

a. Fomentar la gestión proactiva en lugar de la reactiva

b. Concientización de la necesidad de tratar el riesgo en todos los niveles de la organización

c. Mejorar la identificación de oportunidades y amenazas

d. Cumplir con los requisitos normativos

e. Mejorar la gestión empresarial

f. Mejorar la confianza de las partes interesadas

g. Establecer una base fiable para la toma de decisiones

h. Mejorar los controles de mitigación de riesgos

i. Mejorar la eficacia y la eficiencia operacional

j. Aumentar los niveles de seguridad

k. Minimizar las pérdidas

3.7 REQUERIMIENTOS EXIGIDOS POR LA ISO/IEC 27001

Dentro de los requerimientos exigidos por la Norma Internacional ISO 27001 se encuentran los siguientes:

a. Definir el alcance en términos de la organización, su localización, sus activos y tecnologías, incluyendo las exclusiones a que hubiera lugar.

b. Definición de la política del SGSI que incluya un marco general y los objetivos de seguridad de la información de la organización.

c. Definir los criterios mediante los cuales se evaluarán los riesgos.

d. Identificar todos los activos de información que tienen algún valor para la organización, a sus responsables directos y propietarios.

e. Identificar las amenazas relevantes asociadas a los activos identificados.

f. Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas.

g. Identificar el impacto que supondría la pérdida de confidencialidad, integridad y disponibilidad para cada activo.

h. Evaluar el impacto en la organización de un fallo de seguridad que suponga la pérdida de la confidencialidad integridad o disponibilidad de un activo de información.

i. Evaluar la probabilidad de ocurrencia de un fallo de seguridad.

j. Determinar la aceptación del riesgo luego de su evaluación.

k. Dar tratamiento a los riesgos identificados:

    a. Mitigando

    b. Aceptando

    c. Evitando

    d. Transfiriendo

l. Seleccionar los objetivos de control del Anexo A de ISO 27001.

m. Aprobación por parte de la dirección de los riesgos residuales

n. Definir una declaración de aplicabilidad

o. Procurar programas de formación y concienciación

p. Definir procedimientos de monitorización

q. Realizar auditorías internas

r. Revisión del SGSI por parte de la alta gerencia

s. Realizar acciones preventivas y correctivas.

Gráfica 11: Sistemas de Gestión de Seguridad de la Información, Fuente: Ana Cecilia Vargas y Alonso Castro Mattei http://archivo.ucr.ac.cr

3.8 METODOLOGÍAS DE RIESGOS COMO BASE DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

3.8.1 NTC ISO 31000

La norma ISO 31000, establece los principios y directrices para la Gestión de Riesgo en las organizaciones, proporcionando además una guía para los programas de auditorías internas o externas. La implementación de esta norma apoya a las diferentes entidades para aumentar la probabilidad de cumplir con la política y los objetivos del negocio de manera tal que la efectiva aplicación de esta, proporcionen sólidos principios para una gestión eficaz y una óptima gestión empresarial.

Los principales objetivos de la norma ISO 31000 son:

a) Aumentar la probabilidad de mitigación de riesgos.

b) Encaminar a las organizaciones para el cumplimiento de requisitos legales y normativos sobre la gestión de riesgos empresariales.

c) Mejorar el nivel de los Stakeholder para la identificación de amenazas y vulnerabilidades.

d) Minimizar las pérdidas organizacionales mejorando e implementando controles efectivos.

e) Encamina a la organización a la gestión del riesgo más no a la eliminación de estos.

Los principios que establece esta norma para que la gestión del riesgo sea eficaz y los cuales deben poner en práctica las organizaciones son:

a) La gestión del riesgo protege y crea valor.

b) La gestión del riesgo es una parte integral de todos los procesos de la organización.

c) La gestión del riesgo es parte de la toma de decisiones.

d) La gestión del riesgo aborda explícitamente la incertidumbre.

e) La gestión del riesgo es sistemática, estructurada y oportuna.

f) La gestión del riesgo se basa en la mejor información disponible.

g) La gestión del riesgo está adaptada.

h) La gestión del riesgo toma en consideración los factores humanos y culturales.

i) La gestión del riesgo es transparente e inclusiva.

j) La gestión del riesgo facilita la mejora continua de la organización.

La ISO 31000 puede ser aplicada a cualquier tipo de empresa pública o privada, tipo de sector o industria.

Fases:

1 **Comunicar y Consultar:** efectuar la comunicación con las partes involucradas desde el principio de la implementación y en todas las etapas de la misma, ya que esto muestra diferentes percepciones y agregan valor a las decisiones necesarias para la gestión del riesgo.

2 **Establecer el contexto:** definir los parámetros internos y externos relevantes que sirvan como referencia para la gestión particular de los riesgos de la organización.

3 Contexto Externo.

4 Contexto Interno.

5 Contexto del Proceso para la Gestión del Riesgo.

6 Definir los Criterios del Riesgo.

   a) **Valoración del Riesgo:** identificación, análisis y evaluación del riesgo.

   b) **Tratamiento del Riesgo:** definición de los controles necesarios para el nivel de aceptación del riesgo y así mismo la generación de planes aplicables a la prevención y mitigación de los mismos.

7 **Selección de opciones para el tratamiento del riesgo:** preparación e implementación de los planes de tratamiento del riesgo.

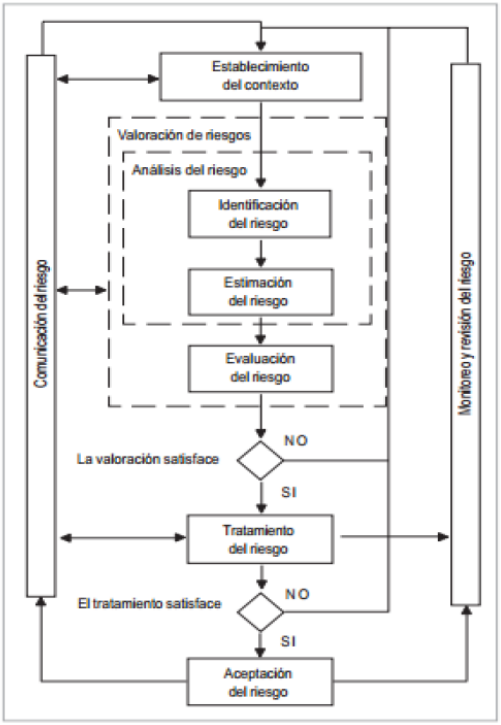
8 **Monitorear y Revisar:** validar la eficacia y eficiencia de los controles y planes de tratamiento implementados para la gestión de riesgos.

9 **Registro del proceso para la Gestión del Riesgo**: durante todo el proceso de la gestión del riesgo es importante llevar el registro de las actividades realizadas y los resultados obtenidos con el fin de implementar mejoras en cada uno de los procesos, las cuales con un análisis detallado apliquen a cada caso.

3.8.2 ISO/IEC 27005

La Norma ISO 27005, forma parte de la familia de ISO 27000 la cual fomenta la seguridad de la información, esta norma, aporta un enfoque para la descripción del proceso de gestión de riesgos de la seguridad de la información proporcionando a los departamentos de TI un marco para la implementación de gestión de riesgos, por medio de acciones asociadas, además apoya conceptos generales empleados en la norma ISO/IEC como tecnología de la información, técnicas de seguridad, sistemas de gestión de seguridad y requisitos.

ISO 27005 aplica a los sistemas de información de todas las organizaciones, por lo tanto, se adapta al enfoque de gestión de riesgos de cualquiera de estas.



Gráfica 12: Mapa de Análisis de Riesgos bajo la norma ISO/IEC 27005. Fuente. ISO (International Standard Organization)

Fases

a) **Identificación de Activos:** un activo es todo aquello que tiene valor para la organización y que, por lo tanto, requiere protección. Para la identificación de los activos se recomienda tener en cuenta que el sistema de información va más allá de hardware y software. La identificación de los activos debe ser detallado, este, debe proporcione información suficiente para la valoración del riesgo. Es necesario identificar al propietario de cada activo, con el fin de asignar responsabilidad sobre este y de ser necesario posteriores rendiciones de cuentas

b) **Valoración de Riesgos en la Seguridad de la Información:** un riesgo es una combinación de las consecuencias que pueden presentar luego de la ocurrencia de un evento indeseado y de su probabilidad de ocurrencia. La valoración del riesgo permite priorizar los riesgos según su nivel de verdad.

c) **Análisis del Riesgo:** Identificado los riesgos, se estudia la posibilidad, consecuencia y factores que contribuyen a la ocurrencia de los mismos, lo anterior para definir los niveles de los riesgos y así poderlos gestionar. Para

la realización del análisis se utilizan varios métodos y puede hacerse de forma cualitativa o cuantitativa

d) **Identificación del riesgo:** esta identificación de los riesgos permite determinar cuál puede ser la causa de la pérdida potencial y entender cómo, dónde y por qué podría ocurrir la pérdida. Se desarrolla a partir de fuentes como: planes estratégicos, planes de acción, reportes de desempeño, presupuestos, riesgos identificados por otras entidades estatales, lluvia de ideas, paneles de expertos cuando la complejidad del proceso de contratación lo exige, análisis DOFA (Debilidades, Oportunidades, Fortalezas y Amenazas), encuestas y cuestionarios. La identificación de riesgos se basa en los riesgos de la gestión de la calidad ya que su desarrollo y plan de ejecución se desarrollan conjuntamente en el análisis de riesgos y la toma de decisiones para la implementación de medidas necesarias que aseguren la información.

e) **Identificación de las amenazas:** una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a las organizaciones. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas. Es recomendable identificar tanto los orígenes de las amenazas accidentales como de las deliberadas. Una amenaza puede tener su origen dentro o fuera de la organización. Las amenazas se deberían identificar genéricamente y por tipo (por ejemplo, acciones no autorizadas, daño físico, fallas técnicas) y, cuando sea adecuado, las amenazas individuales dentro de la clase genérica identificada. Esto significa que ninguna amenaza se pasa por alto, incluidas las inesperadas, pero teniendo en cuenta que el volumen de trabajo requerido es limitado.

f) **Control de Riesgos (políticas):**

a. Realizar jornadas de capacitación al personal sobre el SGSI y medidas a implementar para la protección de la información.

b. Administrar el acceso al sistema de información.

c. Las claves de accesos son personales e intransferibles, por lo tanto, una incorrecta manipulación dará como resultado la sanción a la persona que tenga a nombre la cuenta asociada.

d. Restringir los sitios de navegación que pueden filtrar información.

e. Generar la cultura para que los funcionarios apoyen la confidencial del Sistema de Información.

El proceso de gestión de riesgos de seguridad de la información se compone de:

a) Contexto de creación.
b) Evaluación de riesgos
c) Tratamiento de los riesgos
d) Aceptación del riesgo
e) La comunicación de riesgos
f) Riesgo de control y revisión

3.8.3 Metodología de riegos de MINTIC

El Ministerio de Tecnologías de la Información y las Comunicaciones, MINTIC, desarrolló una guía de gestión de riesgos donde se recogen los aspectos más importantes de las prácticas y documentos de uso libre de manejo de riesgos. La guía se crea con el fin de brindar buenas prácticas para las entidades del estado.

Se aplica a las entidades públicas y privadas que desempeñan funciones públicas y que deban o deseen implementar su SGSI

Las fases de la metodología planteada por el MINTIC (2011) las cuales se encuentran en el documento anexo 6: metodología de gestión del riesgo son:

I. Iniciación: Se comienza la planeación de la creación de un sistema de TI, se documenta el propósito y alcance del sistema. Además, en esta fase se identifican los riesgos y se utilizan para soportar el desarrollo de los requerimientos del sistema, deben incluirse requerimientos de seguridad y las estrategias

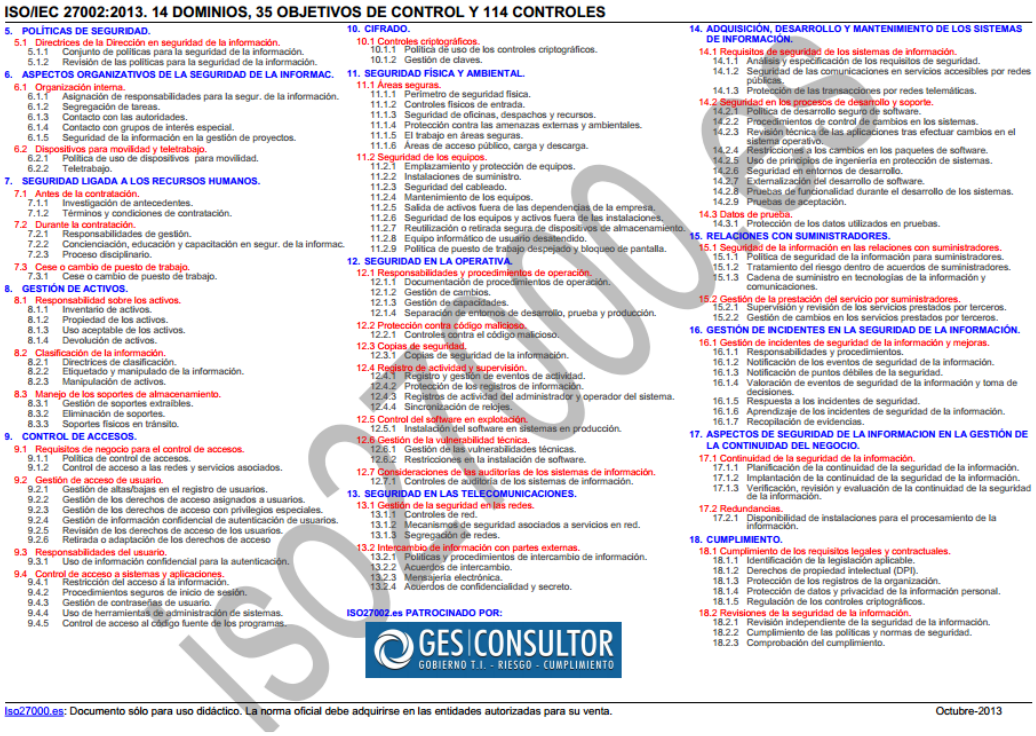
II. Desarrollo o Adquisición: En esta fase se diseña, compra, construye o se desarrolla el sistema de TI. En esta fase, se hace una revisión de los riesgos con el fin de determinar cuáles se deben tener en cuenta y cuales se pueden eliminar.

III. Implementación: En esta fase es importante configurar, activar, probar y verificar las características de seguridad del sistema, tomando decisiones sobre los riesgos identificados.

IV. Operación o mantenimiento: El sistema realiza su función sufriendo varias modificaciones por cambios en el hardware y el software, los procesos, las políticas y los procedimientos organizacionales.

V. Disposición (Retiro): Esta fase comprende la disposición de la información, el hardware y el software ya sea a través del traslado, el archivo, el descarte o la destrucción de la información y la limpieza de hardware y software. Es importante descartar los riesgos que no se necesitan con el fin de asegurar que los riesgos residuales son tratados.

3.8.4 CONTROLES ESTABLECIDOS EN LA ISO/IEC 27002.



ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
5.1 Directrices de la Dirección en seguridad de la información.
5.1.1 Conjunto de políticas para la seguridad de la información.
5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
6.1 Organización interna.
6.1.1 Asignación de responsabilidades para la segur. de la información.
6.1.2 Segregación de tareas.
6.1.3 Contacto con las autoridades.
6.1.4 Contacto con grupos de interés especial.
6.1.5 Seguridad de la información en la gestión de proyectos.
6.2 Dispositivos para movilidad y teletrabajo.
6.2.1 Política de uso de dispositivos para movilidad.
6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
7.1 Antes de la contratación.
7.1.1 Investigación de antecedentes.
7.1.2 Términos y condiciones de contratación.
7.2 Durante la contratación.
7.2.1 Responsabilidades de gestión.
7.2.2 Concienciación, educación y capacitación en segur. de la informac.
7.2.3 Proceso disciplinario.
7.3 Cese o cambio de puesto de trabajo.
7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
8.1 Responsabilidad sobre los activos.
8.1.1 Inventario de activos.
8.1.2 Propiedad de los activos.
8.1.3 Uso aceptable de los activos.
8.1.4 Devolución de activos.
8.2 Clasificación de la información.
8.2.1 Directrices de clasificación.
8.2.2 Etiquetado y manipulado de la información.
8.2.3 Manipulación de activos.
8.3 Manejo de los soportes de almacenamiento.
8.3.1 Gestión de soportes extraíbles.
8.3.2 Eliminación de soportes.
8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
9.1 Requisitos de negocio para el control de accesos.
9.1.1 Política de control de accesos.
9.1.2 Control de acceso a las redes y servicios asociados.
9.2 Gestión de acceso de usuario.
9.2.1 Gestión de altas/bajas en el registro de usuarios.
9.2.2 Gestión de los derechos de acceso asignados a usuarios.
9.2.3 Gestión de los derechos de acceso con privilegios especiales.
9.2.4 Gestión de información confidencial de autenticación de usuarios.
9.2.5 Revisión de los derechos de acceso de los usuarios.
9.2.6 Retirada o adaptación de los derechos de acceso
9.3 Responsabilidades del usuario.
9.3.1 Uso de información confidencial para la autenticación.
9.4 Control de acceso a sistemas y aplicaciones.
9.4.1 Restricción del acceso a la información.
9.4.2 Procedimientos seguros de inicio de sesión.
9.4.3 Gestión de contraseñas de usuario.
9.4.4 Uso de herramientas de administración de sistemas.
9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
10.1 Controles criptográficos.
10.1.1 Política de uso de los controles criptográficos.
10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
11.1 Áreas seguras.
11.1.1 Perímetro de seguridad física.
11.1.2 Controles físicos de entrada.
11.1.3 Seguridad de oficinas, despachos y recursos.
11.1.4 Protección contra las amenazas externas y ambientales.
11.1.5 El trabajo en áreas seguras.
11.1.6 Áreas de acceso público, carga y descarga.
11.2 Seguridad de los equipos.
11.2.1 Emplazamiento y protección de equipos.
11.2.2 Instalaciones de suministro.
11.2.3 Seguridad del cableado.
11.2.4 Mantenimiento de los equipos.
11.2.5 Salida de activos fuera de las dependencias de la empresa.
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
11.2.8 Equipo informático de usuario desatendido.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
12.1 Responsabilidades y procedimientos de operación.
12.1.1 Documentación de procedimientos de operación.
12.1.2 Gestión de cambios.
12.1.3 Gestión de capacidades.
12.1.4 Separación de entornos de desarrollo, prueba y producción.
12.2 Protección contra código malicioso.
12.2.1 Controles contra el código malicioso.
12.3 Copias de seguridad.
12.3.1 Copias de seguridad de la información.
12.4 Registro de actividad y supervisión.
12.4.1 Registro y gestión de eventos de actividad.
12.4.2 Protección de los registros de información.
12.4.3 Registros de actividad del administrador y operador del sistema.
12.4.4 Sincronización de relojes.
12.5 Control del software en explotación.
12.5.1 Instalación del software en sistemas en producción.
12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Gestión de las vulnerabilidades técnicas.
12.6.2 Restricciones en la instalación de software.
12.7 Consideraciones de las auditorías de los sistemas de información.
12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
13.1 Gestión de la seguridad en las redes.
13.1.1 Controles de red.
13.1.2 Mecanismos de seguridad asociados a servicios en red.
13.1.3 Segregación de redes.
13.2 Intercambio de información con partes externas.
13.2.1 Políticas y procedimientos de intercambio de información.
13.2.2 Acuerdos de intercambio.
13.2.3 Mensajería electrónica.
13.2.4 Acuerdos de confidencialidad y secreto.

ISO27002.es PATROCINADO POR:
GES CONSULTOR
GOBIERNO T.I. - RIESGO - CUMPLIMIENTO

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
14.1 Requisitos de seguridad de los sistemas de información.
14.1.1 Análisis y especificación de los requisitos de seguridad.
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
14.1.3 Protección de las transacciones por redes telemáticas.
14.2 Seguridad en los procesos de desarrollo y soporte.
14.2.1 Política de desarrollo seguro de software.
14.2.2 Procedimientos de control de cambios en los sistemas.
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
14.2.4 Restricciones a los cambios en los paquetes de software.
14.2.5 Uso de principios de ingeniería en protección de sistemas.
14.2.6 Seguridad en entornos de desarrollo.
14.2.7 Externalización del desarrollo de software.
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
14.2.9 Pruebas de aceptación.
14.3 Datos de prueba.
14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
15.1 Seguridad de la información en las relaciones con suministradores.
15.1.1 Política de seguridad de la información para suministradores.
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
15.2 Gestión de la prestación del servicio por suministradores.
15.2.1 Supervisión y revisión de los servicios prestados por terceros.
15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
16.1 Gestión de incidentes de seguridad de la información y mejoras.
16.1.1 Responsabilidades y procedimientos.
16.1.2 Notificación de los eventos de seguridad de la información.
16.1.3 Notificación de puntos débiles de la seguridad.
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
16.1.5 Respuesta a los incidentes de seguridad.
16.1.6 Aprendizaje de los incidentes de seguridad de la información.
16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
17.1 Continuidad de la seguridad de la información.
17.1.1 Planificación de la continuidad de la seguridad de la información.
17.1.2 Implantación de la continuidad de la seguridad de la información.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
17.2 Redundancias.
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
18.1 Cumplimiento de los requisitos legales y contractuales.
18.1.1 Identificación de la legislación aplicable.
18.1.2 Derechos de propiedad intelectual (DPI).
18.1.3 Protección de los registros de la organización.
18.1.4 Protección de datos y privacidad de la información personal.
18.1.5 Regulación de los controles criptográficos.
18.2 Revisiones de la seguridad de la información.
18.2.1 Revisión independiente de la seguridad de la información.
18.2.2 Cumplimiento de las políticas y normas de seguridad.
18.2.3 Comprobación del cumplimiento.

ISO27000

Iso27000.es: Documento sólo para uso didáctico. La norma oficial debe adquirirse en las entidades autorizadas para su venta. Octubre-2013

Gráfica 13: Controles establecidos en norma ISO 27002. Fuente ISO/IEC 27002:2013

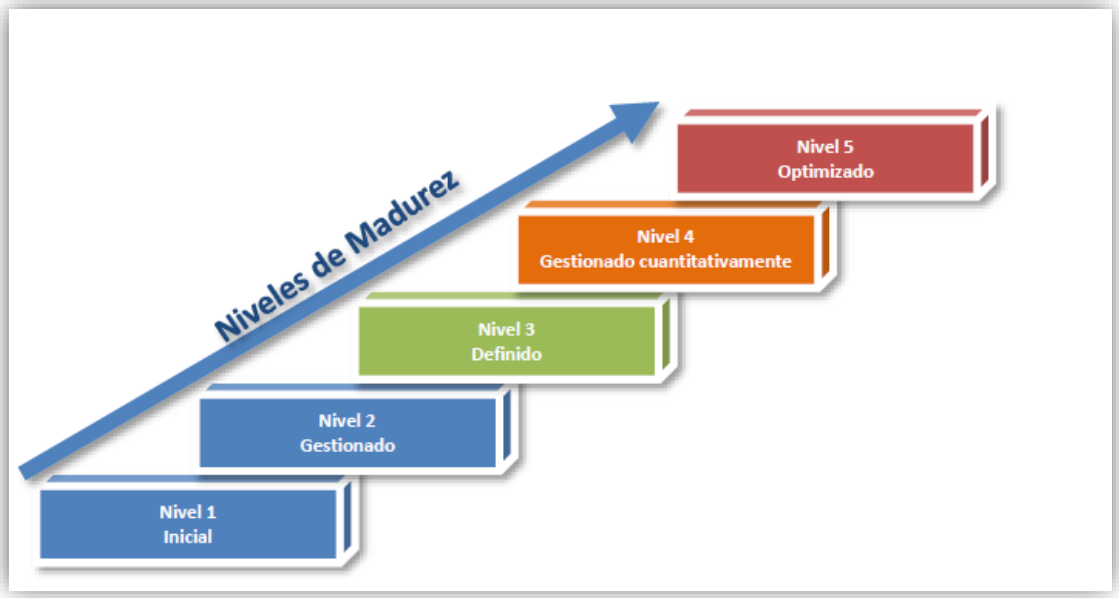
3.9 MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El modelo de seguridad y privacidad de la información es un documento generado por el Ministerio de Tecnología de la Información y Vive Digital Colombia en el cual contiene los “lineamientos, políticas, normas, procesos e instituciones que proveen y promueven la puesta en marcha, supervisión, mejora y control de la implementación del modelo, así como a la implementación de la Estrategia de Gobierno en Línea, establecida en manual GEL” (MINTIC & Vive Digital Colombia, 2015, pág. 8)

Dentro del Modelo de Seguridad y Privacidad de la Información, en el capítulo II – Modelo de Madurez, se observan niveles de madurez, para el progreso permanente de la seguridad y privacidad de la información al interior de la organización, Estos requerimientos, se identifican, se clasifican y se priorizan, como parte del proceso de la gestión de la seguridad y privacidad de la información.

El modelo de madurez permite medir el grado de madurez en el que se encuentran las Entidades, determinando la brecha actual existente, logrando determinar un plan de trabajo que permita dar cumplimiento a los parámetros establecidos en cada nivel.

A continuación, muestran los niveles que conforman el modelo de madurez



Gráfica 14 Niveles de Madurez Fuente Modelo de Seguridad y Privacidad de la Información MINTIC

A continuación, se observa los requerimientos de cada uno de los niveles de madurez con sus respectivas metas

Nivel	Descripción
Inicial	En este nivel se encuentran las Entidades, que aún no cuentan con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información.
Gestionado	En este nivel se encuentran las Entidades, en las cuales existen procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentran gestionados dentro del componente de planificación del MSPI.
Definido	En este nivel se encuentran las Entidades que tiene documentado, estandarizado y aprobado por la dirección, el modelo seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Gestionado cuantitativamente	En este nivel se encuentran las Entidades, que cuenten con métricas, indicadores y realizan auditorías al modelo de seguridad y privacidad de la información, recolectando información para establecer la efectividad de los controles.
Optimizado	En este Nivel se encuentran las Entidades, en donde existe un mejoramiento continuo del modelo de seguridad y privacidad de la información, retroalimentación cualitativa del modelo.

Gráfica 15 requerimientos y metas de cada uno de los niveles de grado de madurez Fuente Modelo de Seguridad y Privacidad de la Información MINTIC

A continuación puede visualizar el paralelo entre los niveles y los controles del modelo de seguridad y privacidad de la información

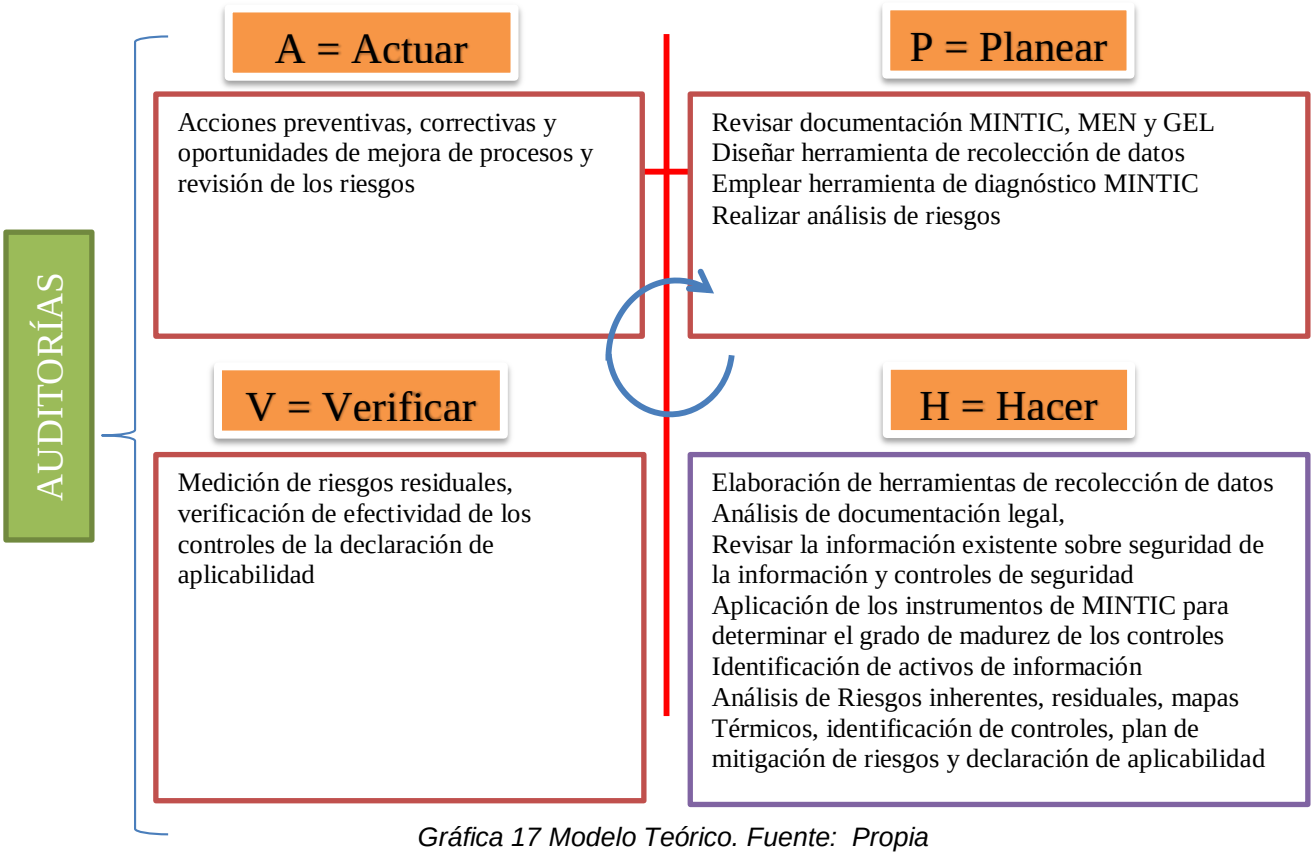
NIVEL	Controles Modelo de Seguridad y Privacidad de la Información
Inicial	**8. GESTION DE ACTIVOS** 8.2 Clasificación de la Información
Gestionado	**5. POLITICA DE SEGURIDAD** 5.1 Directrices de la Dirección en seguridad de la información. **6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN** 6.1 Organización interna. 6.2 Dispositivos para movilidad y teletrabajo. **8. GESTIÓN DE ACTIVOS** 8.1 Responsabilidad sobre los activos. **12. SEGURIDAD EN LA OPERATIVA.** 12.2 Protección contra código malicioso. 12.3 Copias de seguridad. 12.6 Gestión de la vulnerabilidad técnica. **16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.** 16.1 Responsabilidades y procedimientos. **17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.** 17.1.1 Planificación de la continuidad de la seguridad de la información.
Definido	**7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.** 7.1 Antes de la contratación. 7.2 Durante la contratación. 7.3 Cese o cambio de puesto de trabajo. **9. CONTROL DE ACCESOS.** 9.1 Requisitos de negocio para el control de accesos. 9.3 Responsabilidades del usuario. **11. SEGURIDAD FÍSICA Y AMBIENTAL** 11.1 Áreas seguras 11.2 Seguridad de los equipos. **12. SEGURIDAD EN LA OPERATIVA.** 12.1 Responsabilidades y procedimientos de operación.

	12.5 Control del software en explotación. **13. SEGURIDAD EN LAS TELECOMUNICACIONES.** 13.1 Gestión de la seguridad en las redes. 13.2 Intercambio de información con partes externas. **14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.** 14.1 Requisitos de seguridad de los sistemas de información. 14.2 Seguridad en los procesos de desarrollo y soporte. 14.3 Datos de prueba. **16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.** 16.2 Notificación de los eventos de seguridad de la información. 16.1.3 Notificación de puntos débiles de la seguridad. 16.1.7 Recopilación de evidencias. **17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.** 17.1.2 Implantación de la continuidad de la seguridad de la información. **15. RELACIONES CON SUMINISTRADORES** 15.1 Seguridad de la información en las relaciones con suministradores. 15.2 Gestión de la prestación del servicio por suministradores.
Gestionado Cuantitativamente	**9. CONTROL DE ACCESOS.** 9.2 Gestión de acceso de usuario. 9.4 Control de acceso a sistemas y aplicaciones **10. CIFRADO** 10.1 Controles Criptográficos **12. SEGURIDAD EN LA OPERATIVA.** 12.7 Consideraciones de las auditorías de los sistemas de información. 12.4 Registro de actividad y supervisión. **16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.** 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones. 16.1.5 Respuesta a los incidentes de seguridad. **18. CUMPLIMIENTO.** 18.1 Cumplimiento de los requisitos legales y contractuales.
Optimizado	**18. CUMPLIMIENTO** 18.2 Revisiones de la seguridad de la información. **16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.** 16.1.6 Aprendizaje de los incidentes de seguridad de la información. **17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.** Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

Gráfica 16 Paralelo entre los niveles y los controles del modelo de seguridad y privacidad de la información Fuente Modelo de Seguridad y Privacidad de la Información MINTIC

4. MODELO TEÓRICO

De acuerdo a lo establecido en el modelo teórico se considera que una de las metodologías pertinentes de adoptar para la ejecución del proyecto, es la metodología de Deming (Plan, Do, Check, Act) debido a su referente de mejora continua, permitiendo cumplir con el objetivo de este proyecto de diagnosticar el grado de madurez de los controles de seguridad establecidos en la norma NTC ISO /IEC 27001:2013 para las Instituciones educativas del sector público de la comuna universidad de la ciudad de Pereira, teniendo claro lo anterior se inicia con las fases del modelo PHVA



Gráfica 17 Modelo Teórico. Fuente: Propia

FASE DE PLANEAR

Se compone de las siguientes actividades:

1. Definir los instrumentos que serán utilizados para la recolección de información que permitirá diagnosticar las brechas de cumplimiento normativo con relación a la norma NTC ISO/IEC 27001:2013.

2. Identificación de los componentes legales provenientes del Ministerio de Tecnologías de la Información y las comunicaciones – MINTIC, Ministerio de Educación Nacional – MEN, Estrategia Gobierno en Línea.

3. Identificación de las pruebas de penetración que serán empleadas para verificar la vulnerabilidad de los sistemas de información con lo que cuentan las Instituciones de Educación Básica de la Comuna Universidad.

4. Analizar la metodología para el análisis de riesgos propuesta por NIST SP 800-60 e ISO 31000

Se inicia la fase de planeación con la identificación de los procesos o actividades necesarias para dar cumplimiento a dicha fase, luego se determinó la necesidad de realizar una búsqueda y revisión de cada uno de los documentos legales provenientes por el Ministerio de Tecnología de la Información (MINTIC), Ministerio de Educación Nacional (MEN) y Estrategia de Gobierno en Línea (GEL), al realizar el análisis a toda la documentación se identificó un instrumento de diagnóstico el cual permitía medir el grado de madurez de los controles, pero para poder aplicarlo se debía plasmar en una herramienta ofimática que nos permitiese aplicarlo y generar los resultados pertinentes, al igual era necesario contar con un instrumento para definir los riesgos obtenidos durante todo el proceso de recolección de información.

FASE DE HACER

1. Diseñar las herramientas para la recolección de información empleando Microsoft Excel de tal manera que se facilite su aplicación y tabulación, tanto para la herramienta de diseño propio como la suministrada por el Ministerio de las Tecnologías de la Información y las Comunicaciones

2. Análisis de los componentes legales y su convergencia en torno a la seguridad de la información.

3. Aplicación de los instrumentos de recolección de información en las IEDS de la Comuna Universidad de la ciudad de Pereira.

4. Identificación, clasificación y determinación de la criticidad de los activos de información con los que cuenta el sujeto de estudio en cual se llevará a cabo el proceso de validación del modelo.

5. Identificación de los escenarios de riesgos.

6. Calificación de los riesgos inherentes en cada escenario de riesgo para la confidencialidad, integridad y disponibilidad en consonancia con la criticidad de los activos catalogados.

7. Generación de los mapas de temperatura de los riesgos inherentes

8. Identificación de los controles de la Norma NTC ISO/IEC 27001:2013 que serán empleados de acuerdo a los riesgos analizados.

9. Determinación del plan de mitigación de riesgos.

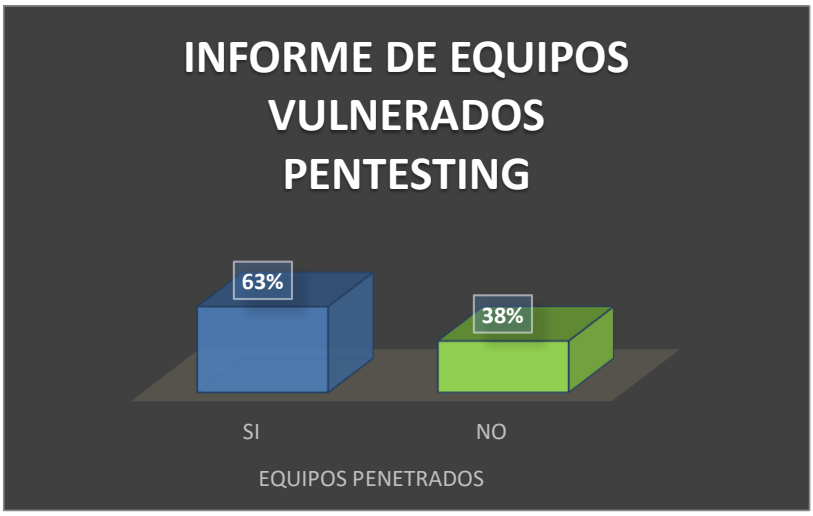
10. Propuesta de la declaración de aplicabilidad.

11. Generación de la documentación requerida por la Norma NTC ISO/IEC 27001:2013

Para iniciar con todo el desarrollo del proyecto, se evidenció en la planeación, la necesidad de construir los instrumentos para la recolección de la información tanto para medir el grado de madurez de los controles, como para identificar los riesgos y los activos físicos y tecnológicos existentes en cada una de las instituciones de la Comuna Universidad.

Al realizar la construcción de los instrumentos se procedió a visitar cada una de las instituciones recolectando la información suficiente para medir el grado de madurez de los controles, los riesgos y los activos antes mencionados, también se empleó pruebas de penetración empleando Kali Linux, mediante el uso de nmap -SP se verificaron los dispositivos conectados a la red, encontrando visibilidad de todos los

equipos, posteriormente se realizó un mapeo de puertos vulnerables mediante nmap -sS -sV encontrando el puerto 139 y 445 disponibles para el test de penetración. Se empleó el comando msfconsole para generar la penetración a través de los puertos identificados.



Gráfica 18 Resultado del Test de penetración en los equipos del área administrativa de la IED sujeto de estudio. Fuente: Propia

Teniendo toda la información recolectada, se procedió analizar cada uno de los instrumentos empleados, generando un informe del estado en el que se encuentra cada una de las instituciones de la Comuna Universidad, luego se realizó un consolidado de los informes para sacar un estado general de la Comuna Universidad, acto seguido se continuo con los otros instrumentos de activos y de riesgos, identificando los riesgos encontrados, para luego determinar los riesgos inherentes, generar las actividades necesarias y así concluir los riesgos residuales, también se realizó un análisis exhaustivo a todas las normativas legales que rigen el sector educativo, con el fin de determinar los controles normativos que deben ser cumplidas por las instituciones educativas, con todo lo anterior se pudo determinar los mapas térmicos, identificación de controles, plan de mitigación de riesgos y por última la construcción de la declaración de aplicabilidad

FASE DE VERIFICAR

1. Calificación de los riesgos residuales en cada escenario de riesgo para la confidencialidad, integridad y disponibilidad en consonancia con la criticidad de los activos catalogados.

2. Generación de los mapas de temperatura de los riesgos residuales.

3. Diagnóstico final de brechas mediante la aplicación de los instrumentos empleados para el diagnóstico inicial.

4. Ajustes a la declaración de aplicabilidad.

Es importante verificar y medir los controles generados para mitigar los riesgos, permitan cerrar las brechas y con ellos generar más seguridad a los activos de información, también es importante verificar que los controles de seguridad de la norma, se ajuste a los controles que por ley debe cumplir las instituciones educativas de la Comuna Universidad de la Ciudad de Pereira.

FASE DE ACTUAR

1. Formulación de acciones preventivas, correctivas y oportunidades de mejora.

2. Revisión de escenarios de riesgo.

Al determinar cada uno de los riesgos y aplicarse los controles necesarios que los neutralicé, con el fin de mitigar el impacto que se puede presentar: Se realiza una serie de recomendaciones preventivas con el fin de mejorar los procesos, dichas recomendaciones están relacionadas al final de este documento.

5. INFORME DE RESULTADO

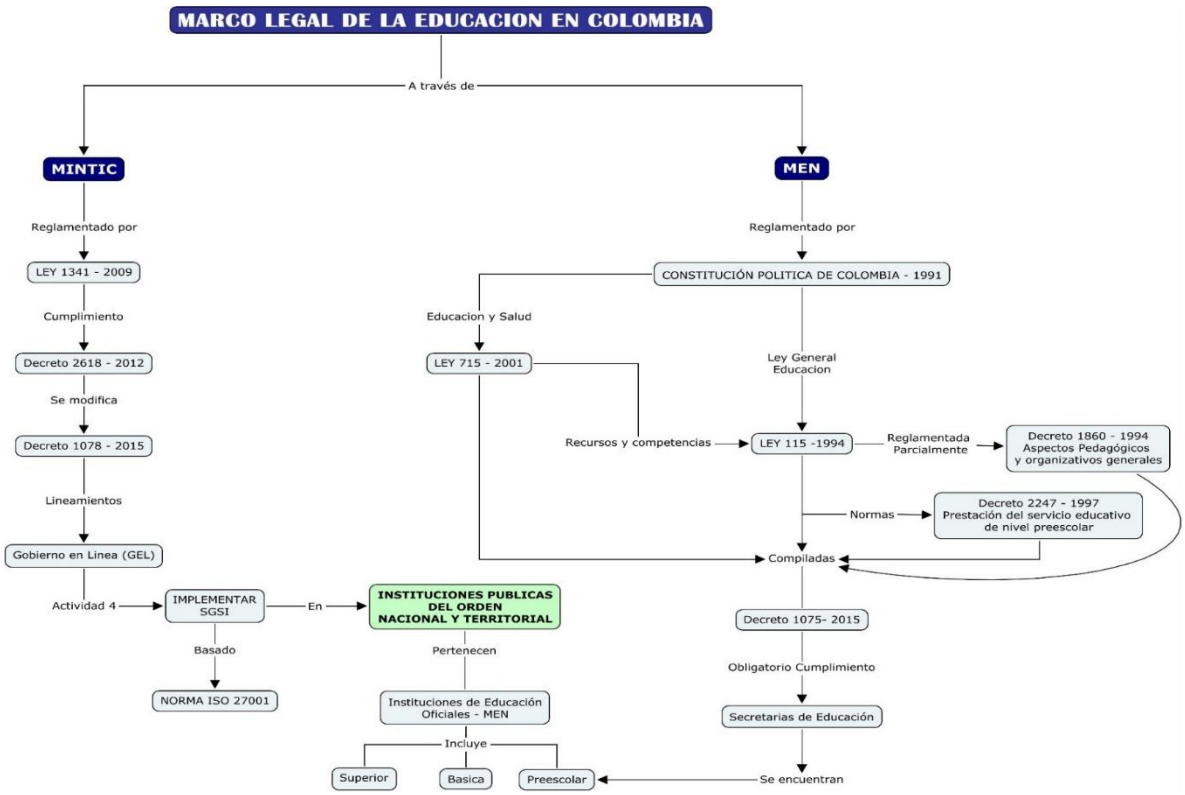
5.1 ANÁLISIS DEL MARCO LEGAL DE LA EDUCACIÓN EN COLOMBIA

Luego de realizar un análisis de la normativa legal de la educación en Colombia, es importante mencionar por separado las normativas que rigen cada uno de los ministerios tanto de tecnología, como el de educación, para al final mencionar el punto en que convergen.

El marco legal que rige el Ministerio de Tecnología de la Información y las Comunicaciones es todo lo relacionado con el auge informático, la evolución y la necesidad de incursionar la tecnología en todos los campos incluyendo el de la educación, pero al generarse todo ese desarrollo tecnológico que conlleva estar a la vanguardia generando múltiples beneficios, también es importante conocer los riesgos de seguridad que se generan, haciendo vulnerable la organización y que deja expuesta la organización, poniendo en riesgo el activo más importante de toda entidad, “la información”. Apalancando la creación de disposiciones legales que exijan a todas las entidades del estado implementar acciones tendientes a la reducción de los riesgos generados por la inclusión de dichas tecnologías en la cotidianidad de sus actividades productivas, una de las disposiciones es la estrategia de gobierno en línea GEL reglamentada mediante el decreto 1078, de tal manera que se garantice la confidencialidad, seguridad y disponibilidad de la información, alineándose con la norma internacional ISO 27001:2013, que contiene los debes normativos y los controles para realizar un implementación de un sistema de Gestión de Seguridad de la Información, para realizar dicha implementación se hacer necesario, diagnosticar el grado de madurez de controles de seguridad de la norma en cada una de las instituciones.

El marco legal que rige el Ministerio de Educación Nacional, el cual se inicia desde la constitución política de Colombia, menciona que la educación en Colombia es un derecho fundamental de todos los niños, además de mencionar que el estado, la familia y la sociedad son los responsables de que los niños a partir de los 5 años accedan a la educación iniciando con un año de preescolar y nueve de educación básica, la ley 715, 115 y los decretos 1860 y 2247 son normativas que rigen la educación en Colombia, en el cual se decreta los niveles de educación los deberes y derechos a los que están sujetos los niños en Colombia en cuanto lo concerniente a la educación e incluso se menciona que es fundamental salvaguardar y mantener confidencialidad con toda la documentación de los menores de edad que se encuentran en cada una de las instituciones educativas.

Al mencionar por separado las normativas que contemplan cada uno de los Ministerios, existe un punto en el que se relacionan los dos y es la información, como resultado del análisis legal de Colombia en cuanto a la seguridad de la información y al contexto educativo y la preservación y cuidado de la información de los niños y niñas se genera el siguiente mapa conceptual que muestra la convergencia de la jurisprudencia emanada de cada ministerio con la obligatoriedad del cumplimiento de GEL



Gráfica 19 Descripción del marco legal en Colombia, fuente: propia

5.2 DIAGNÓSTICO DEL ESTADO ACTUAL DE LAS INSTITUCIONES EDUCATIVAS DE EDUCACIÓN PREESCOLAR DE LA COMUNA UNIVERSIDAD

El presente documento pretende diagnosticar el estado del grado de madurez de los controles de las cuatro Instituciones Educativas, siendo dos de ella instituciones con mayor población a las otras dos que son escuelas de la comuna universidad de la ciudad de Pereira, teniendo como base el instrumento puesto a disposición del público por el Ministerio de Tecnologías de Información y Comunicación - MINTIC.

La audiencia de la guía Encuesta Diagnóstico del Modelo de Seguridad y Privacidad de la información son entidades del estado: del orden nacional y de orden territorial, así como proveedores de servicios de Gobierno en línea, que deseen adoptar el Modelo en el marco de la estrategia de gobierno en línea , (MINTIC, 2015, 6).

En el presente documento se analizan gráfica y numéricamente los resultados arrojados por el instrumento de análisis de información en cada uno de los grados de madurez adoptados por el modelo propuesto por el MINTIC (planeación, implementación, gestión y mejora continua), con el objetivo de generar una base que permita “identificar qué acciones ha desarrollado y cuales hace falta para poder avanzar en el marco del Modelo de Seguridad y Privacidad de la Información”, (MINTIC, 2015, 7).

Tablas para la interpretación de resultados

La guía encuesta Diagnóstico del Modelo de Seguridad y Privacidad de la Información para las entidades del estado, propone las siguientes tablas para la interpretación de resultados en cada una de las fases planteadas por el MINTIC.

- **Fase planeación – limites nivel inicial/Gestionado**

Tabla 8. Tabla para interpretación de resultados fase planeación – límites nivel inicial/gestionado. Fuente: MINTIC, 2015

Limites para las alertas para el Nivel Inicial / Gestionado		
Nivel de Cumplimiento	**Limite Inferior**	**Limite Superior**
Crítico	0	85
Intermedio	86	125
Suficiente	126	210
FASE PLANEACIÓN		

En esta fase se tienen en cuenta los siguientes tópicos:

- Contexto organizacional
  - Establecer y documentar el alcance y la política
  - Establecer procedimientos, roles y responsabilidades dentro del SGSI
- Liderazgo
  - Asignación de recursos
  - Procedimientos de control documental del MSPI (Modelo de Seguridad y Privacidad de la Información)
- Planificación
  - Inventario de activos de información
- Soporte
  - Acciones para tratar riesgos y oportunidades de seguridad de la información
  - Toma de conciencia

- **Fase de implementación – limites nivel definido**

Tabla 9. Tabla para interpretación de resultados fase de implementación – límites nivel definido. Fuente: MINTIC, 2015

Limites para las alertas para el Nivel Definido		
Nivel de Cumplimiento	**Limite Inferior**	**Limite Superior**
Crítico	0	87
Intermedio	88	147
Suficiente	147	245
FASE DE IMPLEMENTACIÓN		

En esta fase se tienen en cuenta los siguientes tópicos:

- Planificación y control operacional
    - Divulgación de las políticas de seguridad y privacidad de la información
    - El comité directivo divulga, las medidas de seguridad y privacidad de la información que deberán ser tomadas para la conservación de la información
- Plan de tratamiento del riesgo
    - Lista de chequeo de requerimientos de seguridad
    - Elaboración del plan de tratamiento del riesgo (Quién, cómo y cuándo)
    - Implementación de controles
    - Seguimiento
- Gestión de recursos y procedimientos implementados para la asignación de recursos financieros
    - Asignación de presupuesto para la seguridad de la información
- Gestión de recursos y procedimientos implementados para la asignación de recursos humanos

- Perfiles y experiencia del personal (descripción) para cada rol o función
- Inventario de habilidades del personal disponible (experiencia existente)
- Procedimientos para la asignación del personal según las funciones
- Procedimientos para la contratación de personal
- Implementación del plan y estrategia de transición de IPV4 a IPV6

➢ **Fase de gestión – límites para el nivel gestionado cuantitativamente**

Tabla 10. Tabla para la interpretación de resultados fase de gestión – límites para el nivel gestionado cuantitativamente. Fuente: MINTIC, 2015

Limites para las alertas para el Nivel Gestionado Cuantitativamente		
Nivel de Cumplimiento	**Limite Inferior**	**Limite Superior**
Crítico	0	28
Intermedio	29	47
Suficiente	48	80
FASE DE GESTIÓN		

En esta fase se tienen en cuenta los siguientes tópicos:

- Plan de seguimiento, evaluación y análisis del MSPI
  - Acciones realizadas y los resultados de la implementación del SGSI
- Auditoría interna
  - Monitoreo a la ejecución de la política, los planes y estándares de la SI
- Plan de tratamiento de riesgos
  - Revisión y aprobación por la alta dirección

- **Fase de mejora continua – límites para el nivel optimizado**

Tabla 11. Tabla para la interpretación de resultados fase de mejora continua – límites para el nivel optimizado. Fuente: MINTIC, 2015

Limites para las alertas para el Nivel Optimizado		
Nivel de Cumplimiento	**Limite Inferior**	**Limite Superior**
Crítico	0	31
Intermedio	32	53
Suficiente	54	90
FASE DE MEJORA CONTINUA		

En esta fase se tienen en cuenta los siguientes tópicos:

- Plan de seguimiento, evaluación y análisis para el MSPI
  - Acciones realizadas y los resultados de la implementación del SGSI
- Revisión y aprobación por la alta dirección
  - Auditoría interna
  - Comunicación de resultados y plan de mejoramiento
  - Revisión y aprobación por la alta dirección

.

Análisis de resultados

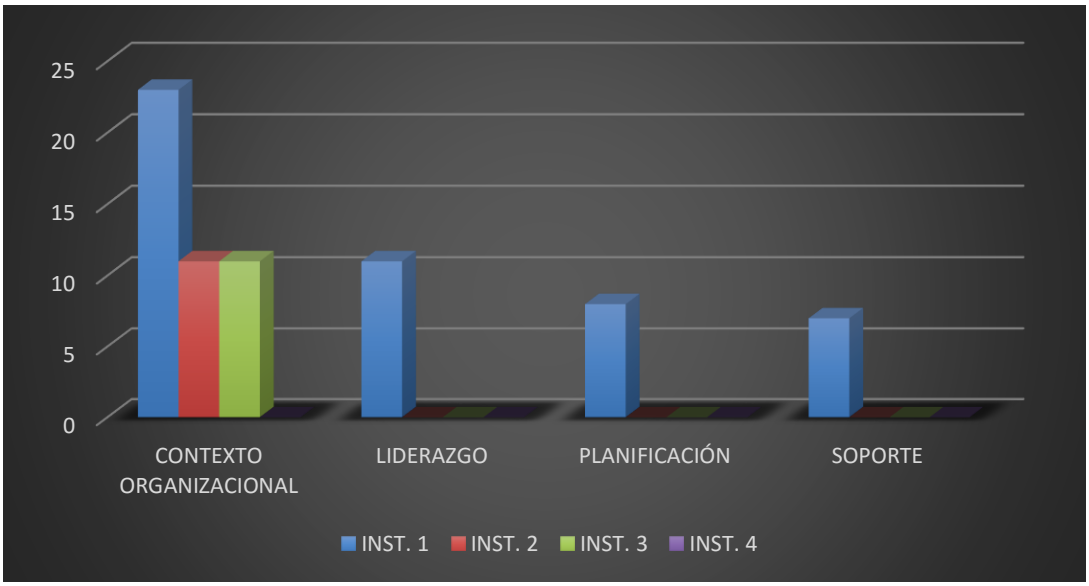
Los resultados se analizaron de acuerdo a la escala de valores que fue establecida por el MINTIC en la guía

Fase planeación – nivel inicial/gestionado

Tabla 12. Fase planeación – nivel inicial/gestionado - valores posibles por pregunta y totales. Fuente MINTIC, 2015

	FASE PLANEACIÓN - INICIAL GESTIONADO																																				
	CONTEXTO ORGANIZACIONAL																LIDERAZGO										PLANIFICACIÓN				SOPORTE							
ESTADO	Establecer y Documentar el Alcance y la Política													Establecer procedimientos, roles y responsabilidades dentro del SGSI				Asignación de Recursos					Procedimientos de Control Documental del MSPI				Inventario de Activos de Información			Acciones para Tratar Riesgos y Oportunidades de Seguridad de la Información					Toma de Conciencia	
	1	2	3	4	5	6	7	8	9	10	11	12	13	1	2	3	4	1	2	3	4	5	1	2	3	4	1	2	3	1	2	3	4	5	1	2
NO TIENE	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
LO TIENE	2	2	3	3	2	3	3	2	2	3	2	1	2	6	6	9	9	7	4	7	5	7	6	8	8	8	8	11	11	5	5	7	7	6	15	15
	TOTAL													TOTAL				TOTAL					TOTAL				TOTAL			TOTAL					TOTAL	
	30													30				30					30				30			30					30	
	GRAN TOTAL																																				
	210																																				

De acuerdo a la tabla anterior para que cada Institución Educativa obtenga el 100% en esta fase debe acumular un total de 210 puntos, al aplicar el instrumento el total de puntos obtenidos en cada una de las instituciones fue de 49, 11, 0 y 11, dando como resultado un 8,5% de acciones llevadas a cabo en esta fase.



Gráfica 20. Representación de los tópicos analizados en la valoración de la fase de planeación – Fuente: elaboración propia.

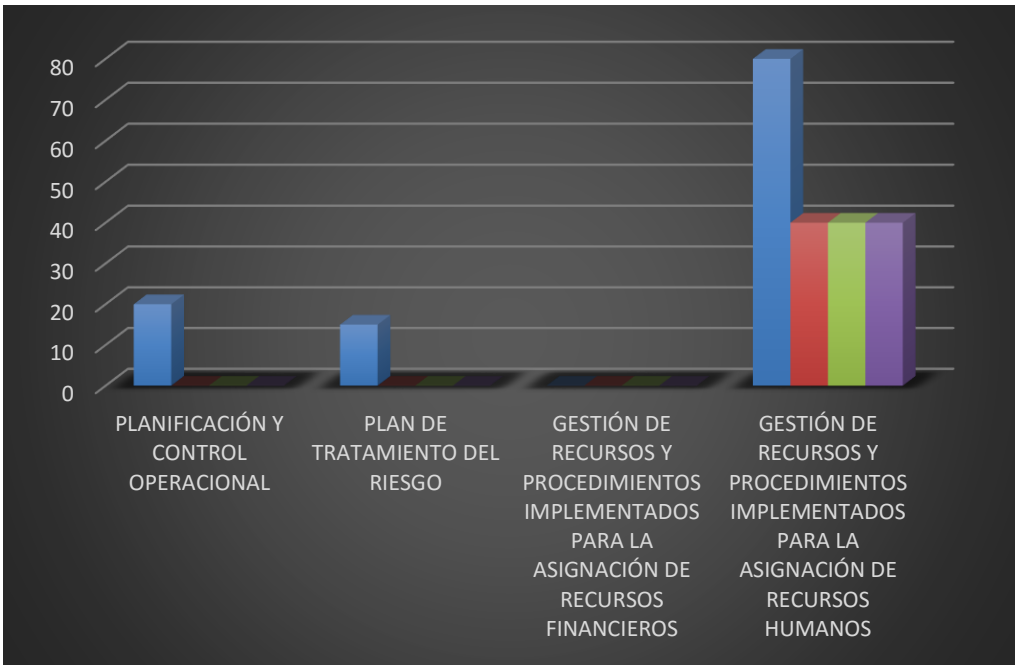
De acuerdo a los resultados totales obtenidos en la comuna universidad en la fase de planeación se obtuvo un promedio de 18 puntos de cumplimiento ubicándose en un nivel de cumplimiento crítico, teniendo en cuenta que el límite inferior es 0 y el superior es 85 conforme a las directrices del instrumento suministrado por MINTIC.

Fase de implementación – nivel definido

En esta etapa cada Institución Educativa debe alcanzar un total de 245 puntos, para obtener el 100% (ver tabla 13), al aplicar el instrumento el total de puntos obtenidos por cada institución fue de 115, 40, 40, 20, dando como resultado un 21,9% de acciones llevadas a cabo en esta fase.

Tabla 13. Fase de implementación – nivel definido. Valores posibles por pregunta y totales. Fuente: MINTIC, 2015

	FASE IMPLEMENTACIÓN - DEFINIDO																					
	PLANIFICACIÓN Y CONTROL OPERACIONAL			PLAN DE TRATAMIENTO DEL RIESGO											GESTIÓN DE RECURSOS Y PROCEDIMIENTOS IMPLEMENTADOS PARA LA ASIGNACIÓN DE RECURSOS	GESTIÓN DE RECURSOS Y PROCEDIMIENTOS IMPLEMENTADOS PARA LA ASIGNACIÓN DE RECURSOS HUMANOS					
ESTADO	Divulgación de las Políticas de Seguridad y Privacidad de la Información	El Comité Directivo Divulga, las Medidas de Seguridad y Privacidad de la Información que Deberan ser Tomadas para la Conservación de	Lista de Chequeo de Requerimientos de Seguridad	Elaboración del Plan de Tratamiento del Riesgo (Quién, Cómo y Cuándo)			Implementación de Controles				Seguimiento		Asignación de Presupuesto para la Seguridad de la Información	Perfiles y Experiencia del Personal (Descripción) para cada Rol o Función	Inventario de Habilidades del Personal Disponible (Experie	Procedimientos para la Asignación del Personal según las Experien	Procedimientos para la Contratación de Personal	Implementación del Plan y Estrategía de Transición de IPV4 a			
	1	1	1	1	2	3	1	2	3	4	1	3	5	1	1	1	1	1			
NO TIENE	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
LO TIENE	10	10	15	10	10	10	7	7	8	8	15	15	20	20	20	20	20	20			
	TOTAL	TOTAL	TOTAL	TOTAL			TOTAL				TOTAL		TOTAL	TOTAL	TOTAL	TOTAL	TOTAL	TOTAL			
	10	10	15	30			30				30		20	20	20	20	20	20			
	GRAN TOTAL																					
	245																					



Gráfica 21. Representación de los tópicos analizados en la valoración de la fase de implementación – Fuente: elaboración propia

La gráfica anterior permite resaltar el tópico que menos influencia tiene en la calificación para la fase de implementación es la gestión de recursos y procedimientos implementados para la asignación de recursos financieros.

De acuerdo a los resultados totales obtenidos en la comuna universidad en la fase de implementación se obtuvo un promedio de 54 puntos de cumplimiento, ubicándose en un nivel de cumplimiento crítico, teniendo en cuenta que el límite inferior es 0 y el superior es 87 conforme a las directrices del instrumento suministrado por MINTIC.

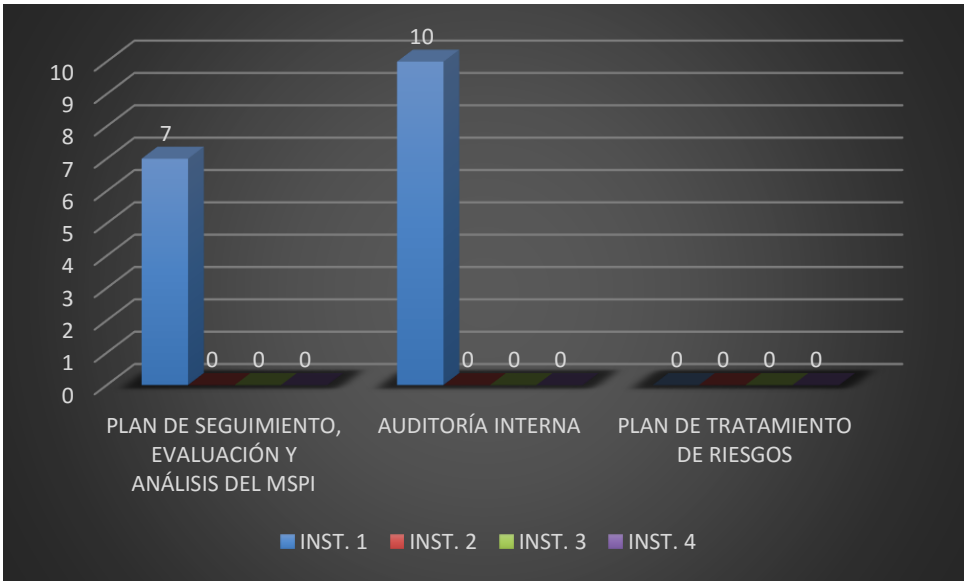
.

Fase de gestión – nivel gestionado cuantitativamente

En esta etapa cada Institución Educativa debe alcanzar un total de 80 puntos, para obtener el 100% (Ver Tabla 14), al aplicar el instrumento el total de puntos obtenidos por cada institución fue de 17,0,0,0, dando como resultado un 1,7% de acciones llevadas a cabo en esta fase.

Tabla 14. Fase de gestión – nivel gestionado cuantitativamente. Valores posibles por pregunta y totales. Fuente: MINTIC, 2015

	FASE GESTIÓN - GESTIONADO CUANTITATIVAMENTE								
	PLAN DE SEGUIMIENTO, EVALUACIÓN Y ANÁLISIS DEL MSPI				AUDITORÍA INTERNA			PLAN DE TRATAMIENTO DE RIESGOS	
ESTADO	Acciones Realizadas y los Resultados de la Implementación del SGSI				Monitoreo a la Ejecución de la Política, los Planes y Estándares de la SI			Asignación de Recursos	
	1	2	3	4	1	2	3	1	2
NO TIENE	0	0	0	0	0	0	0	0	0
LO TIENE	7	7	8	8	10	10	10	10	10
	TOTAL				TOTAL			TOTAL	
	30				30			20	
	GRAN TOTAL								
	80								



Gráfica 22. Representación de los tópicos analizados en la valoración de la fase de gestión – Fuente: elaboración propia

La gráfica anterior permite resaltar el tópico que menos influencia tiene en la calificación para la fase de gestión es el plan de tratamiento de riesgos.

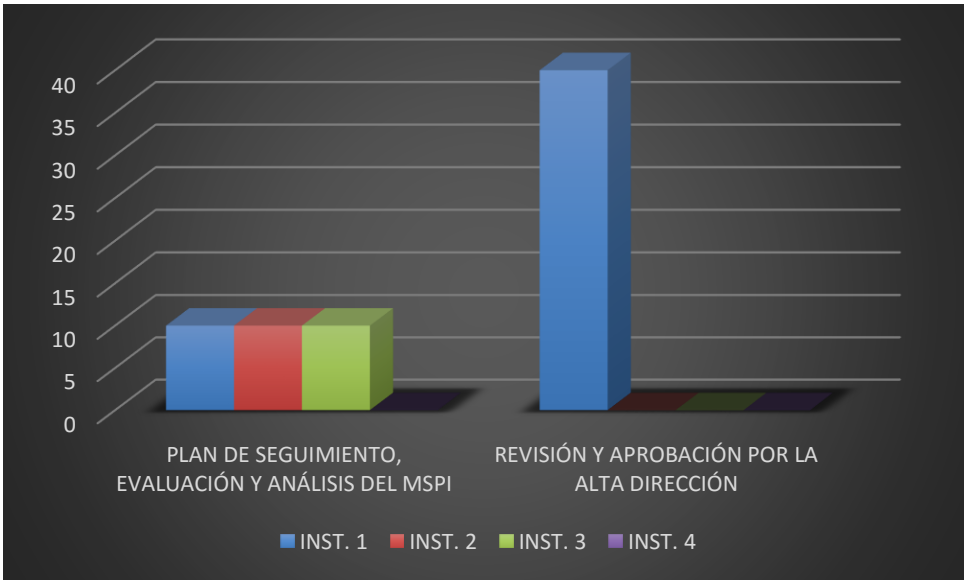
De acuerdo a los resultados totales obtenidos en la comuna universidad en la fase de gestión se obtuvo un promedio de 4 puntos de cumplimiento ubicándose en un nivel de cumplimiento crítico, teniendo en cuenta que el límite inferior es 0 y el superior es 28 conforme a las directrices del instrumento suministrado por MINTIC.

Fase de mejora continua – nivel optimizado

En esta etapa la Institución Educativa debe alcanzar un total de 90 puntos, para obtener el 100% (Ver Tabla 15), al aplicar el instrumento el total de puntos obtenidos por cada institución fue de 50, 10, 10, 0 dando como resultado un 7,1% de acciones llevadas a cabo en esta fase.

Tabla 15. Fase de mejora continua – nivel optimizado. Valores posibles por pregunta y totales. Fuente: MINTIC, 2015

	FASE DE MEJORA CONTINUA - OPTIMIZADO					
	PLAN DE SEGUIMIENTO, EVALUACIÓN Y ANÁLISIS PARA EL MSPI			REVISIÓN Y APROBACIÓN POR LA ALTA DIRECCIÓN		
ESTADO	Acciones Realizadas y los Resultados de la Implementación del SGSI			Auditoría Interna	Comunicación de Resultados y Plan de	Revisión y Aprobación por la Alta Direcciób n
	1	2	3	1	1	1
NO TIENE	0	0	0	0	0	0
LO TIENE	10	10	10	20	20	20
	TOTAL			TOTAL	TOTAL	TOTAL
	30			20	20	20
	GRAN TOTAL					
	90					



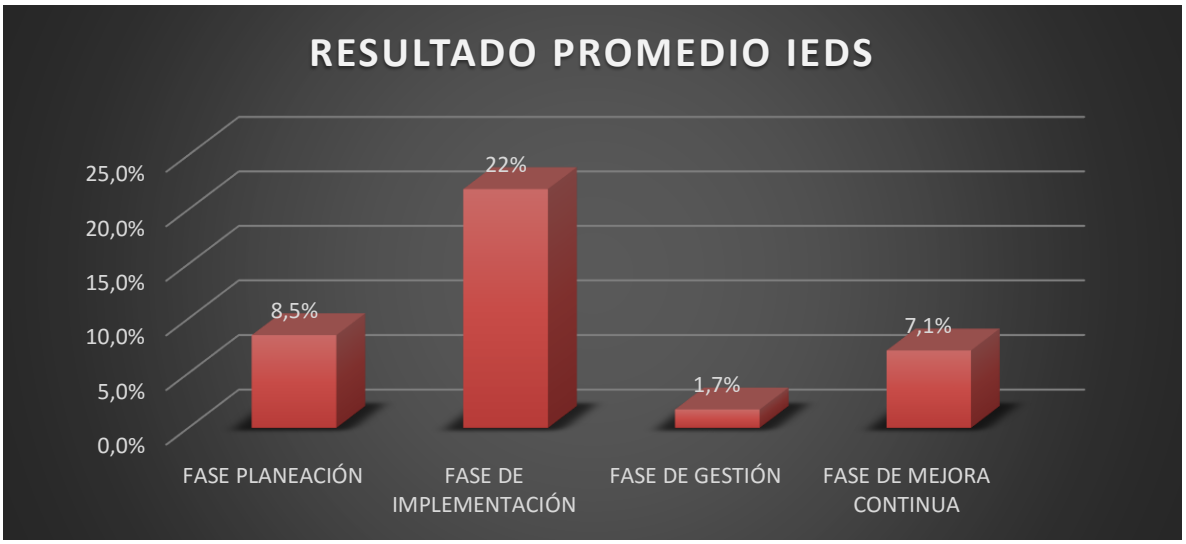
Gráfica 23. Representación de los tópicos analizados en la valoración de la fase de mejora continua – Fuente: elaboración propia

La gráfica anterior permite resaltar el tópico que más influencia tiene en la calificación para la fase de mejora continua es la revisión y aprobación por la alta dirección.

De acuerdo a los resultados totales obtenidos en la comuna universidad en la fase de mejora continua se obtuvo un promedio de 18 puntos de cumplimiento ubicándose en un nivel de cumplimiento crítico teniendo en cuenta que el límite inferior es 0 y el superior es 31 conforme a las directrices del instrumento suministrado por MINTIC.

Conclusión del informe final de resultados

Al observar los resultados arrojados, y siendo consecuentes con los datos arrojados por las instituciones educativas de la comuna universidad, la comuna en general se encuentra en el grado de madurez inicial, debido a que los resultados arrojados por cada uno de los niveles, se evidenció que las instituciones educativas se ubicaron en un nivel de cumplimiento crítico



Gráfica 24 Resultado promedio del diagnóstico realizado a las IEDS Fuente: Propia

Tabla 16 Resultado del grado de madurez de las instituciones de la comuna universidad Fuente: Propia

Limites para las alertas para el Nivel Inicial / Gestionado			
Nivel de Cumplimiento	**Limite Inferior**	**Limite Superior**	**Resultado IEDS**
Crítico	0	85	8,5%
Intermedio	86	125	
Suficiente	126	210	
FASE PLANEACIÓN			

Limites para las alertas para el Nivel Definido			
Nivel de Cumplimiento	**Limite Inferior**	**Limite Superior**	**Resultado IEDS**
Crítico	0	87	22%
Intermedio	88	147	
Suficiente	147	245	
FASE DE IMPLEMENTACIÓN			

Limites para las alertas para el Nivel Gestionado Cuantitativamente			
Nivel de Cumplimiento	**Limite Inferior**	**Limite Superior**	**Resultado IEDS**
Crítico	0	28	1,7%
Intermedio	29	47	
Suficiente	48	80	
FASE DE GESTIÓN			

Limites para las alertas para el Nivel Optimizado			
Nivel de Cumplimiento	**Limite Inferior**	**Limite Superior**	**Resultado IEDS**
Crítico	0	31	7,1%
Intermedio	32	53	
Suficiente	54	90	
FASE DE MEJORA CONTINUA			

5.3 DETERMINACIÓN DEL ALCANCE

De conformidad con lo establecido en el numeral 4.3 de la norma ISO/IEC 27001:2013, en cuanto al alcance; es necesario resaltar que el actual proyecto cubre el área administrativa de las instituciones educativas de nivel preescolar de carácter oficial, la cual está conformada por las siguientes dependencias, en la que se puede observar igualmente el responsable del levantamiento de información:

Tabla 17 Alcance del SGSI de la Institución Fuente: Propia

DEPENDENCIA/SERVICIOS	RESPONSABLE
Coordinación académica y disciplinaria **Procesos disciplinarios, asignación de salones, permisos, información de asignación disciplinaria, almacenamiento información de seguimiento académico.**	Liliana Grajales
Secretaria académica **Administración y custodia de información de soporte académico de los estudiantes matriculas, actas, certificados**	Mónica León Zuluaga
Psicología **Administración y custodia de información de estudiantes con acompañamiento sicológico**	Liliana Grajales
Rectoría **Administración y mantenimiento de bienes inmuebles, de la infraestructura tecnológica, de la estructura organizacional, difusión de información institucional, procesos de rendición de informes a la Secretaría de Educación Municipal**	Mónica León Zuluaga
Secretaría de rectoría **Administración y mantenimiento de bienes inmuebles, de la infraestructura tecnológica, de la estructura organizacional, difusión de información institucional, procesos de rendición de informes a la Secretaría de Educación Municipal**	Mónica León Zuluaga
Tesorería **Administración y custodia de la información de las inversiones presupuestales de la institución**	Liliana Grajales
Sala de juntas **Sistema de información de vigilancia de las áreas comunes de la institución educativa**	Mónica León Zuluaga Liliana Grajales

5.4 ESTRUCTURA ORGANIZACIONAL DE LA SEGURIDAD DE LA INFORMACIÓN

Gráfica 25 Estructura organizacional de la seguridad de la Información Fuente: Propia

5.5 IDENTIFICACIÓN DE ACTIVOS TECNOLÓGICOS

Para la identificación y clasificación de los activos se tuvo en cuenta la siguiente tabla con el fin determinar la criticidad del activo dentro del área administrativa de la institución educativa

Tabla 18 Factores determinando la criticidad de los activos Fuente propia

FACTORES PARA DETERMINAR LA CRITICIDAD DE LOS ACTIVOS		
Criterio	**Factor Afectado**	**Pregunta**
Disponibilidad	Financiero	¿Si el activo o la información que se gestiona a través de él no están disponibles puede generar pérdidas económicas para la entidad?
	Legal	¿Si el activo o la información que se gestiona a través de él no están disponibles puede generar sanciones legales de entes de control o demandas de terceros?
	Imagen	¿Si el activo o la información que se gestiona a través de él no están disponibles puede afectar la imagen de la entidad?
Integridad	Financiero	¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede generar pérdidas económicas para la entidad?
	Legal	¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede generar sanciones de entes de control?
	Imagen	¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede afectar la imagen de la entidad?
Confidencialidad	Financiero	¿Su divulgación no autorizada puede relevar información sensible de la empresa requerida para la toma de decisiones estratégicas y financieras?
	Legal	¿Su divulgación no autorizada puede afectar el cumplimiento de regulaciones impartidas por entes de control o puede generar demandas de terceros?
	Imagen	¿Su divulgación no autorizada puede afectar la imagen de la entidad?

Cada uno de los activos fue puntuado para determinar el grado de criticidad para la institución educativa y poder tener el insumo que permita realizar el cálculo de los riesgos inherentes basados en los tres criterios Confiabilidad, Integridad y disponibilidad, el valor máximo de cada ítem evaluado por criterio es 1, dando un total de 3 punto como máximo para cada criterio.

De acuerdo a la valoración dada a cada activo para los criterios se determina la criticidad de acuerdo a la siguiente tabla:

Tabla 19 Nivel de criticidad de los activos de la información Fuente propia

Nivel de criticidad de los activo de información		
Criterio de Evaluación	**Valor criticidad activo**	**Nivel criticidad**
La gestión del activo compromete en un alto grado la integridad y/o confidencialidad y/o disponibilidad de la información de la Institución	>=3	Alto
La gestión del activo compromete en un nivel medio la integridad y/o confidencialidad y/o disponibilidad de la información.	2	Medio
La gestión del activo compromete en un nivel bajo la integridad y/o confidencialidad y/o disponibilidad de la información de la institución	1	Bajo
La gestión del activo no compromete la integridad, confidencialidad y disponibilidad de la información de la empresa	0	No aplica

Listado de activos incluida la calificación de la criticidad para los procesos organizacionales de la institución:

Tabla 20 Criticidad de los activos Fuente propia

CRITICIDAD DE LOS ACTIVOS FISICOS

N° ACTIVO	PROCESO	TIPO DOCUMENTO	NOMBRE DEL DOCUMENTO	Valoración nivel de criticidad del activo												Nivel de criticidad	OBSERVACIONES
				Confidencialidad			Integridad			Disponibilidad							
				Financiero	Legal	Imagen	Financiero	Legal	Imagen	Financiero	Legal	Imagen	Confidencialidad	Integridad	Disponibilidad	Valor Total	
1	Coordinación Disciplinaría	Formato	Reporte de conducta Inapropiada del estudiante	1	1	1	1	1	1	1	1	1	3	3	3	9	ALTO	Se encontró la información detrás de un archivador, se evidencia registro fotográfico
2	Coordinación Académica	6 archivadores de 4 gavetas, 5 metálico y 1 de madera	Providencia tarde - 3 archivadores metálicos	1	1	1	1	1	1	1	1	1	3	3	3	9	NO APLICA	No tiene placa de inventario, están marcados por los grados escolares
3	Coordinación Académica	Documentos varios, bolsas cuadernos y carpetas	1 archivador de madera	1	1	1	1	1	1	1	1	1	3	3	3	9	NO APLICA	
4	Coordinación Académica	información varia de la julita y marco Fidel Suarez	2 archivadores metálicos	1	1	1	1	1	1	1	1	1	3	3	3	9	ALTO	tiene hojas de vida de los docentes y administrativos, diplomas

6	Coordinación Académica	archivador movible de 3 cuerpos, en la parte trasera, 5 entrepaños ALA 3	información del liceo Pereira desde el año 1958, información del colegio Juvenal Cano Moreno desde 1970	1	1	1	1	1	1	1	1	1	3	3	3	9	ALTO	hay un sensor de movimiento, en un punto ciego, en la parte superior hay información del Colegio Remigio Antonio Cañarte del año 2013, hay una carpeta con información de registro de notas y certificación de notas del año 2013 del remigio Antonio
7	Coordinación Académica	ala 3 parte delante	información del Rafael Uribe Uribe y de la julita	1	1	1	1	1	1	1	1	1	3	3	3	9	ALTO	
8	Coordinación Académica	Ala 2 parte trasera	información del Rafael Uribe, colegio Hildardo Castaño Orozco Corosito desde el año 1991, Benjamín herrera	1	1	1	1	1		1	1	1	3	2	3	8	ALTO	se encontró una bolsa como marbetes usados, otra bolsa con muchos ganchos de legajar
9	Coordinación Académica	ala 2 parte delantera	información del Rafael Uribe desde 1965 y juvenal cano por años desde 1994	1	1	1	1		1	1	1	1	3	2	3	8	ALTO	
10	Coordinación Académica	ala 1	información del colegio Benjamín Herrara, Liceo Pereira, complejo educativo la julita y marco Fidel Suarez	1	1	1	1	1	1	1	1	1	3	3	3	9	ALTO	

CRITICIDAD DE LOS ACTIVOS TÉCNOLOGICO

N° ACTIVO	PROCESO	TIPO ACTIVO	COD INVENTARIO INTERNO	SERIAL	ESTADO	MODELO	MARCA	Valoración nivel de criticidad del activo												Nivel de criticidad	OBSERVACIONES
								Confidencialidad			Integridad			Disponibilidad								
								Financiero	Legal	Imagen	Financiero	Legal	Imagen	Financiero	Legal	Imagen	Confidencialidad	Integridad	Disponibilidad	Valor Total		
1	Coordinación Disciplinaría	BAFLES	NO TIENE	CNPV03275076	BUENO	AR550A	COMPAQ	0	0	0	0	0	0	0	0	0	0	0	0	0	NO APLICA	Se encontró detrás de un archivador
2	Coordinación Disciplinaría	MOUSE	NO TIENE	BZC5VF	BUENO	MSU0923	HP	0	0	0	0	0	0	0	0	0	0	0	0	0	NO APLICA	
3	Coordinación Disciplinaría	TECLADO	NO TIENE	BZC17W	BUENO	KU-0841	HP	0	0	0	0	0	0	0	0	0	0	0	0	0	NO APLICA	
4	Coordinación Disciplinaría	DVD	NO TIENE		BUENO	VTA-83006	VTA	0	0	0	0	0	0	0	0	0	0	0	0	0	NO APLICA	Serial despegado
5	Coordinación Disciplinaría	COMPUTADOR	NO TIENE	3CR03314FH	BUENO	100-5010LA	HP OMNI 100	0	1	1	1	1	1	1	1	1	2	3	3	8	ALTO	Es un todo en uno
6	Coordinación Disciplinaría	IMPRESORA	NO TIENE	CNB2716847	REGULAR	HP LASERJET 1020	HP	0	0	0	0	0	0	0	0	0	0	0	0	0	NO APLICA	la carcasa de la parte superior de la impresora está quebrada
7	Coordinación Disciplinaría	ESTABILIZADOR	VARIOS 0012	N/A	BUENO	PR-1000	ARTELECTRO	0	0	0	0	0	0	0	0	0	0	0	0	0	NO APLICA	Capacidad de 1000 voltios, con 4 puertos de conexión

8	Coordinación Académico	BAFLES	NO TIENE	YK8094009539	BUENO	SP-F200	GENIUS	0	0	0	0	0	0	0	0	0	0	0	0	0	NO APLICA	
9	Coordinación Académico	UPS	NO TIENE	N/A	BUENO	PS1200	UNITEC	0	0	0		0	0	0	0	0	0	0	0	0	NO APLICA	
10	Coordinación Académico	PBX	NO TIENE	R002212	BUENO	TEM824LA	PANASONIC	0	0	0	1	1	1	1	1	1	0	3	3	6	ALTO	Tapa trasera que cubre cables suelta
11	Coordinación Académico	IMPRESORA LASER	NO TIENE	VND3G45473	BUENO	LASERJET 1102	HP	0	0	0	0	0	0	0	0	0	0	0	0	0	NO APLICA	
12	Coordinación Académico	ESTABILIZADOR	NO TIENE		BUENO	R1000	ELECTROLINEC	0	0	0	0	0	0	0	0	0	0	0	0	0	NO APLICA	
13	Coordinación Académico	TELEFONO (CONMUTADOR)			BUENO	KXT7730X	PANASONIC	0	0	0	0	0	0	0	0	0	0	0	0	0	NO APLICA	
14	Coordinación Académico	TECLADO	2	N/A	BUENO		DELL	0	0	0	0	0	0	0	0	0	0	0	0	0	NO APLICA	
15	Coordinación Académico	CPU			BUENO		JANUS	0	1	1	1	1	1	1	1	1	2	3	3	8	ALTO	
16	Coordinación Académico	MONITOR	NO TIENE	ET78807191026	BUENO	E2200HDA LCD	BENQ	0	1	1	1	1	1	1	1	1	2	3	3	8	ALTO	
17	Coordinación Académico	MOUSE	NO TIENE	120900250	BUENO	HM5010	PC SMART	0	0	0	0	0	0	0	0	0	0	0	0	0	NO APLICA	
18	Servidor	PORTATIL	NO TIENE	2053241	BUENO		COMPUMAX	1	1	1	1	1	1	1	1	1	3	3	3	9	ALTO	
19	Secretaría de Rectoría	MONITOR	NO TIENE	ET89806379026	BUENO	E2200HDA LCD	BENQ	0	1	1	1	1	1	1	1	1	2	3	3	8	ALTO	
20	Secretaría de Rectoría	TORRE	NO TIENE	EQ S/PCS100066	BUENO	NO TIENE	PC SMART	0	1	1	1	1	1	1	1	1	2	3	3	8	ALTO	

21	Secretaría de Rectoría	MOUSE	NO TIENE	165127506245	BUENO	NO TIENE	GENIUS	0	0	0	0	0	0	0	0	0	0	0	0	0	NO APLICA	
22	Secretaría de Rectoría	TECLADO	NO TIENE	CN-0DJ415-71616-6AH-0MHY	BUENO	SK-8115	DELL	0	0	0	0	0	0	0	0	0	0	0	0	0	NO APLICA	TODO SE BORRO
23	Secretaría de Rectoría	IMPRESORA	NO TIENE	CNBKS20434	BUENO	LASERJET 1200	HP	0	0	0	0	0	0	0	0	0	0	0	0	0	NO APLICA	
24	Secretaría de Rectoría	TELEFONO	NO TIENE	BORRADO	BUENO	KX-T2310	PANASONIC	0	0	0	0	0	0	0	0	0	0	0	0	0	NO APLICA	Se borró el serial
25	Secretaría de Rectoría	IMPRESORA	NO TIENE	NO TIENE	BUENO	FS1016MFP	KYOCERA	0	0	0	0	0	0	0	0	0	0	0	0	0	NO APLICA	
26	Tesorería	COMPUTADOR	NO TIENE	4CS0030KJP	BUENO	MS200	HP	0	1	1	1	1	1	1	1	1	2	3	3	8	ALTO	un todo en uno
27	Tesorería	MOUSE	NO TIENE	X63396806593	BUENO	GM-04003A	GENIUS	0	0	0	0	0	0	0	0	0	0	0	0	0	NO APLICA	
28	Tesorería	TECLADO	NO TIENE	WE2492066556	BUENO	K639	BB-06XE	0	0	0	0	0	0	0	0	0	0	0	0	0	NO APLICA	
29	Tesorería	TELEFONO	SIN CODIGO	7AABF849671	BUENO	KX-T2310	PANASONIC	0	0	0	0	0	0	0	0	0	0	0	0	0	NO APLICA	
30	Tesorería	IMPRESORA LASER	NO TIENE	Z7C2B8GD3A01D9R	BUENO	ML-2165W	SAMSUNG	0	0	0	0	0	0	0	0	0	0	0	0	0	NO APLICA	
31	Rectoría	ROUTER	NO TIENE	270873420	BUENO	DPC2320	CISCO	0	0	0	0	0	0	1	0	1	0	0	2	2	ALTO	
32	Rectoría	SWITCHE	NO TIENE	NO TIENE	BUENO	ENH916P-NWY	ENCORE	0	0	0	0	0	0	1	0	1	0	0	2	2	MEDIO	16 PUERTOS

5.6 DETERMINACIÓN DE RIESGOS

De acuerdo al estudio realizado se determinan los siguientes escenarios de riesgos:

Tabla 21 Escenario de Riesgo Fuente Propia

1	Problemas legales por pérdida de información
2	Falta de reacción apropiada y oportuna en la ocurrencia de un incidente
3	Obsolescencia en los controles de seguridad de capacitación
4	La ejecución de un proyecto puede alterar la Confiabilidad, disponibilidad e integridad de los activos críticos
5	Acceso a información crítica mediante el uso de dispositivos móviles
6	Tratamiento inadecuado de la información debido a la falta de claridad en las condiciones de trabajo
7	Tratamiento inadecuado de la información crítica por desconocimiento de la políticas y procedimientos
8	No contar con un proceso debidamente documentado, que de las directrices para adelantar procesos disciplinarios en caso de violación en la seguridad de la información
9	Acceso de información privilegiado por parte de un empleado que ha sido promovido
10	Perdida de activos por falta de un inventario actualizado
11	Imposibilidad en la asignación de responsabilidades en caso de pérdida o daño de activos
12	Uso inadecuado de los activos por parte de los propietarios de los mismos
13	Pérdida de los activos por falta de trazabilidad en préstamo.
14	Sanciones legales por tratamiento indebido de la información
15	Imposibilidad de recuperación de la información necesario o requerida para adelantar procesos críticos de prestación del servicio
16	Manejo inadecuado de activos por carencia de una adecuada clasificación de la información
17	Copia no autorizada de información crítica de la organización
18	Robo de medios

19	Pérdida de la integridad y disponibilidad de información almacenada en medios, causa por un tratamiento indebido o no autorizado por parte de las personas que las custodian o de terceros
20	Acceso de personal no autorizado a CPD
21	Acceso de personal no autorizado a información crítica por medio de las conexiones de red
22	Acceso a los activos de información con privilegios disonantes con el perfil del usuario
23	Acceso de los activos de información por parte de personal no autorizado
24	Acceso a sistemas de información por deficiencias en los sistemas de autenticación
25	Acceso no autorizado a los sistemas de información
26	Parálisis de los servicios de los sistemas de información por el uso de programas utilitarios
27	Instalación de código no autorizado que afecte negativamente la operación de los sistemas de información
28	Acceso a información privilegiada
29	Intrusión de personas ajenas no autorizadas a las instalaciones físicas
30	Pérdida de activos críticos causado por desastres naturales ataques maliciosos o accidentes
31	Sanciones legales o daño en activos
32	Daños en los equipos por fallas de fluido eléctrico
33	*Daños en los cableados por problemas eléctricos *Interceptación del sistema de registro de estudiantes y tesorería
34	Fallos en la prestación de servicio de tesorería y secretaria académica por problemas en los funcionamientos de los equipos
35	Pérdida de los equipos
36	Pérdida de los equipos o daños cuando se encuentran fuera de la instalación
37	Pérdida de información por falta de copias de seguridad
38	Daños en los equipos
39	Dificultad en la recuperación de información crítica
40	Error en los procedimientos de registro académico por falta de información documentada que especifique las actividades relacionadas con dicho registro
41	Pérdida de integridad de la información en el proceso de registro académico
42	Deficiencias en la atención de la comunidad académica por recursos insuficientes

43	Errores de disponibilidad de la información académica y tesorería por uso de software sin haber realizado pruebas
44	Interceptación de información por código maliciosos instalado con o sin voluntad por el usuario del sistema
45	Perdidas de la continuidad del negocio por daños en los equipos o sistemas de información
46	Problemas en sistemas de información sin resolver por falta de información de trazabilidad
47	Acceso no autorizado a la información de registro
48	Problemas de integridad de información sin resolver por falta de sincronización de los sistemas de información
49	Sanciones legales por software pirata
50	Acceso no autorizado a información crítica
51	Acceso no autorizado a información crítica a través de las redes
52	Acceso no autorizado en los sistemas de información de secretaria académica mediante la explotación de vulnerabilidades
53	Fallos en la prestación del servicio por falta de pruebas
54	Daños en la información original comprometiendo la disponibilidad, integridad y confidencialidad de la información
55	Acceso no autorizado a información crítica
56	Fuga de información de los dicentes por parte de los proveedores que intervienen en los sistemas de información
57	Pérdida de imagen por no atención oportuna por daños en los activos
58	No se presta el servicio de registro académico permanentemente a los usuarios a consecuencia de un desastre natural
59	Ausencia de información crítica redundante que garantice la disponibilidad y la continuidad de los procesos críticos (registro académico y tesorería)
60	Sanciones legales por uso inadecuado de la información de conformidad por lo dispuesto por el MEN
61	Sanciones legales por uso inadecuado de la información de conformidad por lo dispuesto por la legislación de derechos de autor
62	Sanciones legales por uso inadecuado de la información de conformidad por lo dispuesto por el MEN y la ley de habeas data
63	Ausencia de controles alineados a la realidad operativa de la seguridad de la información por falta de revisiones periódicas

5.7 CALIFICACIÓN DEL RIESGO INHERENTE

Se definen los siguientes criterios para la calificación de la probabilidad

Tabla 22 Calificación de probabilidades Fuente Propia

TABLA DE PROBABILIDADES		
VALOR	**PROBABILIDAD**	**DESCRIPCIÒN**
3	ALTO	Más de 10 veces al año o alta probabilidad de ocurrencia
2	MEDIO	Entre 5 y 10 veces al año o mediana probabilidad de ocurrencia
1	BAJO	Menos de 5 veces al año o baja probabilidad de ocurrencia

Para la calificación del impacto potencial se tomaron los criterios establecidos por la Norma NISP 800-60

Tabla 23 Calificación de impacto potencial Fuente NIST SP 800-60 (2008)

IMPACTO POTENCIAL			
	BAJO (1)	**MODERADO (2)**	**ALTO (3)**
CONFIDENCIALIDAD La preservación de las restricciones autorizadas sobre el acceso y divulgación de información, que incluye medios para la protección de la intimidad personal y la propiedad de la información.	la divulgación no autorizada de información podría tener un efecto adverso **limitado** en las operaciones de la organización, los activos de la organización o sus individuos	se podría esperar que la divulgación no autorizada de información tenga un efecto adverso **serio** sobre las operaciones de la organización, los activos de la organización o sus individuos.	la divulgación no autorizada de información podría tener un efecto adverso **grave o catastrófico** en las operaciones de la organización, los activos de la organización, o individuos.
INTEGRIDAD Protección contra la inapropiada modificación o destrucción de información, e incluye garantizar el no repudio y la autenticidad de la información.	La modificación o destrucción no autorizada de información podrían tener un efecto adverso **limitado** en las operaciones de la organización, los activos de la organización o sus individuos	La modificación o destrucción no autorizada de información podrían tener un efecto adverso **serio** en las operaciones de la organización, los activos de la organización o sus individuos	La modificación o destrucción no autorizada de información podrían tener un efecto adverso **grave o catastrófico** en las operaciones de la organización, los activos de la organización o sus individuos

DISPONIBILIDAD Garantizar el acceso oportuno y confiable y uso de la información.	La interrupción del acceso o uso de información o a un sistema de información podría tener un efecto adverso **limitado** en las operaciones de la organización, los activos de la organización, o sus individuos.	La interrupción del acceso o uso de información o a un sistema de información podría tener un efecto adverso **serio** en las operaciones de la organización, los activos de la organización, o sus individuos.	La interrupción del acceso o uso de información o a un sistema de información podría tener un efecto adverso **grave o catastrófico** en las operaciones de la organización, los activos de la organización, o sus individuos.

Tabla 24 Escenarios de riesgos Fuente Propia

CODIGO	ESCENARIO DE RIESGO	PROBABILIDAD	IMPACTO				VULNERABILIDAD INHERENTE			
			C	I	D	TOTAL	C	I	D	T
1	Problemas legales por pérdida de información	3	2	2	2	6	66,67%	66,67%	66,67%	66,67%
2	Falta de reacción apropiada y oportuna en la ocurrencia de un incidente	2	1	1	2	4	22,22%	22,22%	44,44%	29,63%
3	Obsolescencia en los controles de seguridad por falta de capacitación	2	2	2	2	6	44,44%	44,44%	44,44%	44,44%
4	La ejecución de un proyecto puede alterar la Confiabilidad, disponibilidad e integridad de los activos críticos	2	3	3	3	9	66,67%	66,67%	66,67%	66,67%
5	Acceso a información crítica mediante el uso de dispositivos móviles	2	3	0	0	3	66,67%	0,00%	0,00%	22,22%
6	Tratamiento inadecuado de la información debido a la falta de claridad en las condiciones de trabajo	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%
7	Tratamiento inadecuado de la información crítica por desconocimiento de la políticas y procedimientos	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%

8	No contar con un proceso debidamente documentado, que de las directrices para adelantar procesos disciplinarios en caso de violación en la seguridad de la información	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%
9	Acceso de información privilegiado por parte de un empleado que ha sido promovido	2	1	1	1	3	22,22%	22,22%	22,22%	22,22%
10	Perdida de activos por falta de un inventario actualizado	3	2	2	2	6	66,67%	66,67%	66,67%	66,67%
11	Imposibilidad en la asignación de responsabilidades en caso de pérdida o daño de activos	3	2	2	2	6	66,67%	66,67%	66,67%	66,67%
12	Uso inadecuado de los activos por parte de los propietarios de los mismos	2	1	1	1	3	22,22%	22,22%	22,22%	22,22%
13	Pérdida de los activos por falta de trazabilidad en préstamo.	3	2	2	2	6	66,67%	66,67%	66,67%	66,67%
14	Sanciones legales por tratamiento indebido de la información	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%
15	Imposibilidad de recuperación de la información necesario o requerida para adelantar procesos críticos de prestación del servicio	2	2	2	2	6	44,44%	44,44%	44,44%	44,44%
16	Manejo inadecuado de activos por carencia de una adecuada clasificación de la información	2	2	2	2	6	44,44%	44,44%	44,44%	44,44%

17	Copia no autorizada de información crítica de la organización	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%
18	Robo de medios	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%
19	Pérdida de la integridad y disponibilidad de información almacenada en medios, causa por un tratamiento indebido o no autorizado por parte de las personas que las custodian o de terceros	3	3	3	3	3	100,00%	100,00%	100,00%	33,33%
20	Acceso de personal no autorizado a CPD	2	3	3	3	9	66,67%	66,67%	66,67%	66,67%
21	Acceso de personal no autorizado a información crítica por medio de las conexiones de red	3	3	3	3	3	100,00%	100,00%	100,00%	33,33%
22	Acceso a los activos de información con privilegios disonantes con el perfil del usuario	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%
23	Acceso de los activos de información por parte de personal no autorizado	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%
24	Acceso a sistemas de información por deficiencias en los sistemas de autenticación	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%
25	Acceso no autorizado a los sistemas de información	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%

26	Parálisis de los servicios de los sistemas de información por el uso de programas utilitarios	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%
27	Instalación de código no autorizado que afecte negativamente la operación de los sistemas de información	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%
28	Acceso a información privilegiada	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%
29	Intrusión de personas ajenas no autorizadas a las instalaciones físicas	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%
30	Pérdida de activos críticos causado por desastres naturales ataques maliciosos o accidentes	3	3	3	3	3	100,00%	100,00%	100,00%	33,33%
31	Sanciones legales o daño en activos	2	2	2	2	6	44,44%	44,44%	44,44%	44,44%
32	Daños en los equipos por fallas de fluido eléctrico	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%
33	*Daños en los cableados por problemas eléctricos *Interceptación del sistema de registro de estudiantes y tesorería	2	3	3	3	9	66,67%	66,67%	66,67%	66,67%
34	Fallos en la prestación de servicio de tesorería y secretaria académica por problemas en los funcionamientos de los equipos	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%
35	Pérdida de los equipos	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%

36	Pérdida de los equipos o daños cuando se encuentran fuera de las instalaciones	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%
37	Pérdida de información por falta de copias de seguridad	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%
38	Daños en los equipos	3	2	2	2	6	66,67%	66,67%	66,67%	66,67%
39	Dificultad en la recuperación de información crítica	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%
40	Error en los procedimientos de registro académico por falta de información documentada que especifique las actividades relacionadas con dicho registro	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%
41	Pérdida de integridad de la información en el proceso de registro académico	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%
42	Deficiencias en la atención de la comunidad académica por recursos insuficientes	2	1	1	1	3	22,22%	22,22%	22,22%	22,22%
43	Errores de disponibilidad de la información académica y tesorería por uso de software sin haber realizado pruebas	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%
44	Interceptación de información por código maliciosos instalado con o sin voluntad por el usuario del sistema	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%

45	Perdidas de la continuidad del negocio por daños en los equipos o sistemas de información	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%
46	Problemas en sistemas de información sin resolver por falta de información de trazabilidad	2	2	2	2	6	44,44%	44,44%	44,44%	44,44%
47	Acceso no autorizado a la información de registro	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%
48	Problemas de integridad de información sin resolver por falta de sincronización de los sistemas de información	2	1	1	1	3	22,22%	22,22%	22,22%	22,22%
49	Sanciones legales por software pirata	3	2	2	2	6	66,67%	66,67%	66,67%	66,67%
50	Acceso no autorizado a información crítica	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%
51	Acceso no autorizado a información crítica a través de las redes	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%
52	Acceso no autorizado en los sistemas de información de secretaria académica mediante la explotación de vulnerabilidades	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%
53	Fallos en la prestación del servicio por falta de pruebas	3	2	2	2	6	66,67%	66,67%	66,67%	66,67%
54	Daños en la información original comprometiendo la disponibilidad, integridad y confidencialidad de la información	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%

55	Acceso no autorizado a información crítica	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%
56	Fuga de información de los dicentes por parte de los proveedores que intervienen en los sistemas de información	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%
57	Pérdida de imagen por no atención oportuna por daños en los activos	3	1	1	1	3	33,33%	33,33%	33,33%	33,33%
58	No se presta el servicio de registro académico permanentemente a los usuarios a consecuencia de un desastre natural	2	2	2	2	6	44,44%	44,44%	44,44%	44,44%
59	Ausencia de información crítica redundante que garantice la disponibilidad y la continuidad de los procesos críticos (registro académico y tesorería)	3	3	3	3	9	100,00%	100,00%	100,00%	100,00%
60	Sanciones legales por uso inadecuado de la información de conformidad por lo dispuesto por el MEN	3	2	2	2	6	66,67%	66,67%	66,67%	66,67%
61	Sanciones legales por uso inadecuado de la información de conformidad por lo dispuesto por la legislación de derechos de autor	2	2	2	2	6	44,44%	44,44%	44,44%	44,44%

62	Sanciones legales por uso inadecuado de la información de conformidad por lo dispuesto por el MEN y la ley de habeas data	3	2	2	2	6	66,67%	66,67%	66,67%	66,67%
63	Ausencia de controles alineados a la realidad operativa de la seguridad de la información por falta de revisiones periódicas	3	2	2	2	6	66,67%	66,67%	66,67%	66,67%

5.8 MAPA DE RIESGO INHERENTE

Tabla 25 Criterios de aceptabilidad del riesgo inherente Fuente propia

CRITERIOS DE ACEPTABILIDAD DEL RIESGO		
IDENTIFICACIÓN	**CRITERIO**	**DESCRIPCIÓN**
	ACEPTABLE	Vulnerabilidad < 25%
	TOLERABLE	Vulnerabilidad entre el 25 y el 50%
	INACEPTABLE	Vulnerabilidad superior al 50%

Tabla 26 Mapa de riesgos confidencialidad inherente Fuente Propia

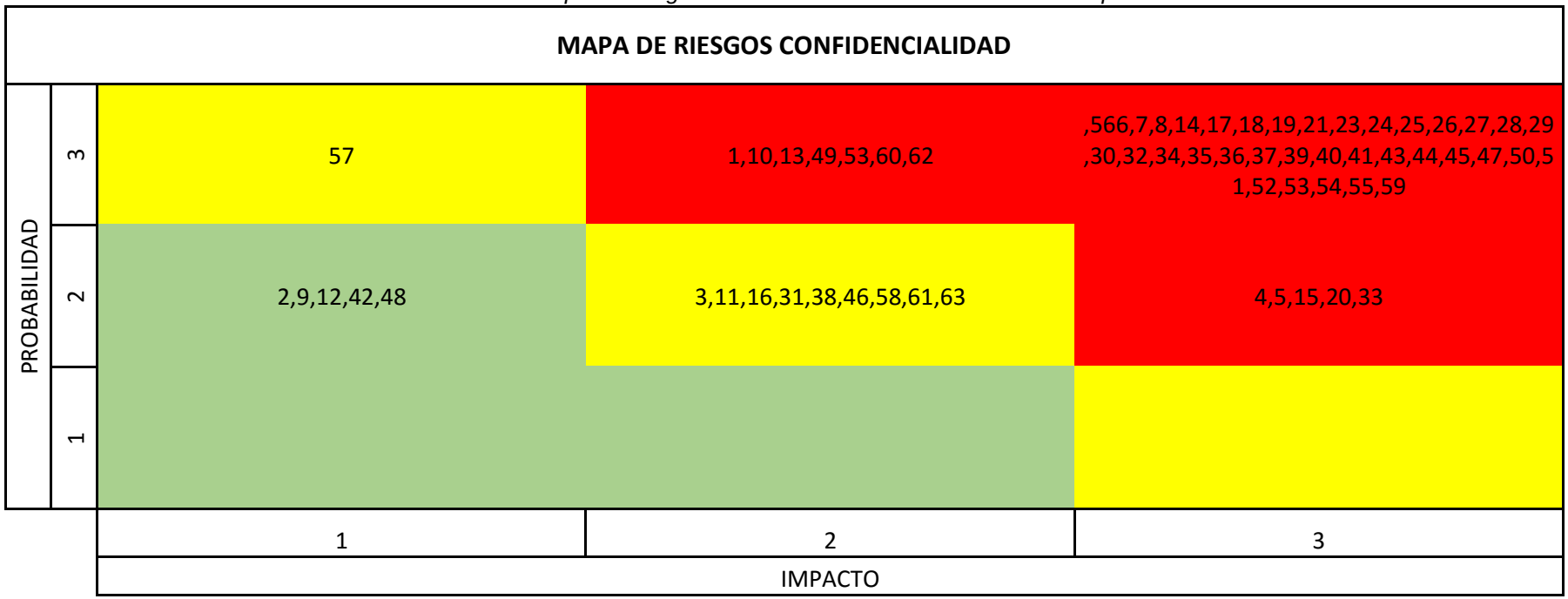


Tabla 27 Mapa de Riesgos Integridad inherente Fuente Propia

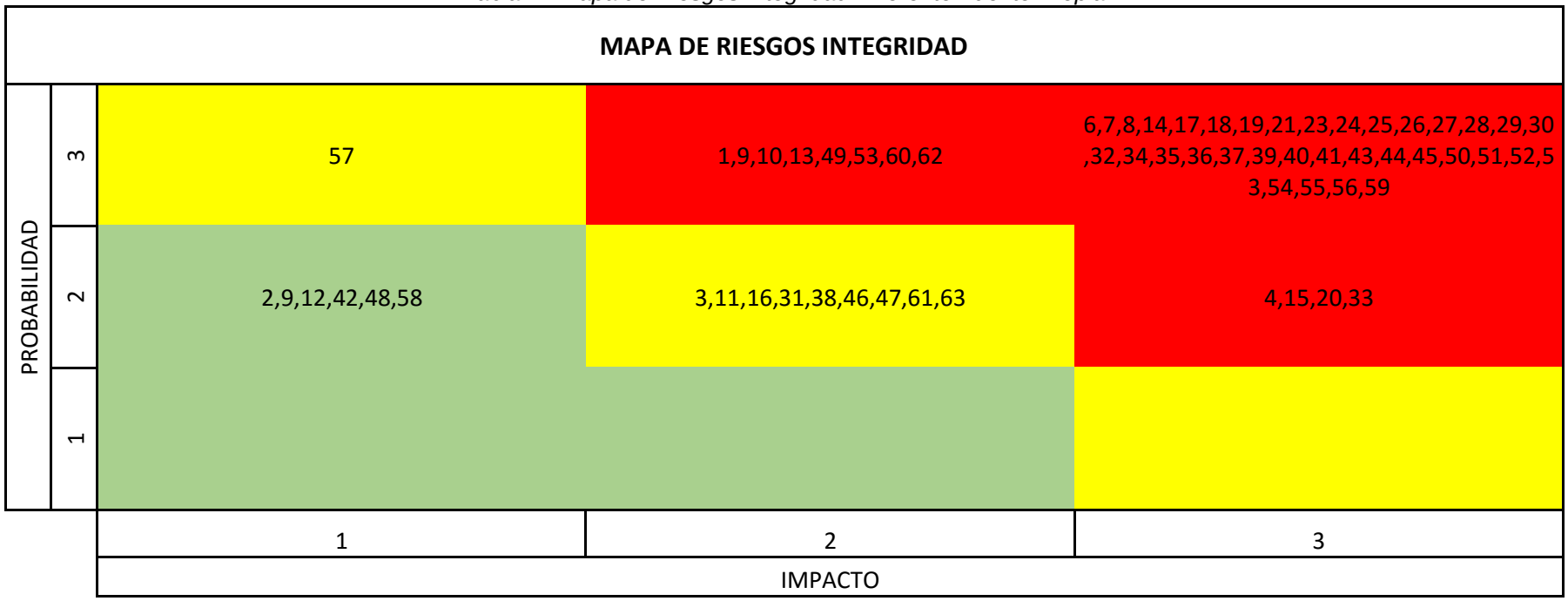


Tabla 28 Mapa de riesgos disponibilidad inherente Fuente Propia

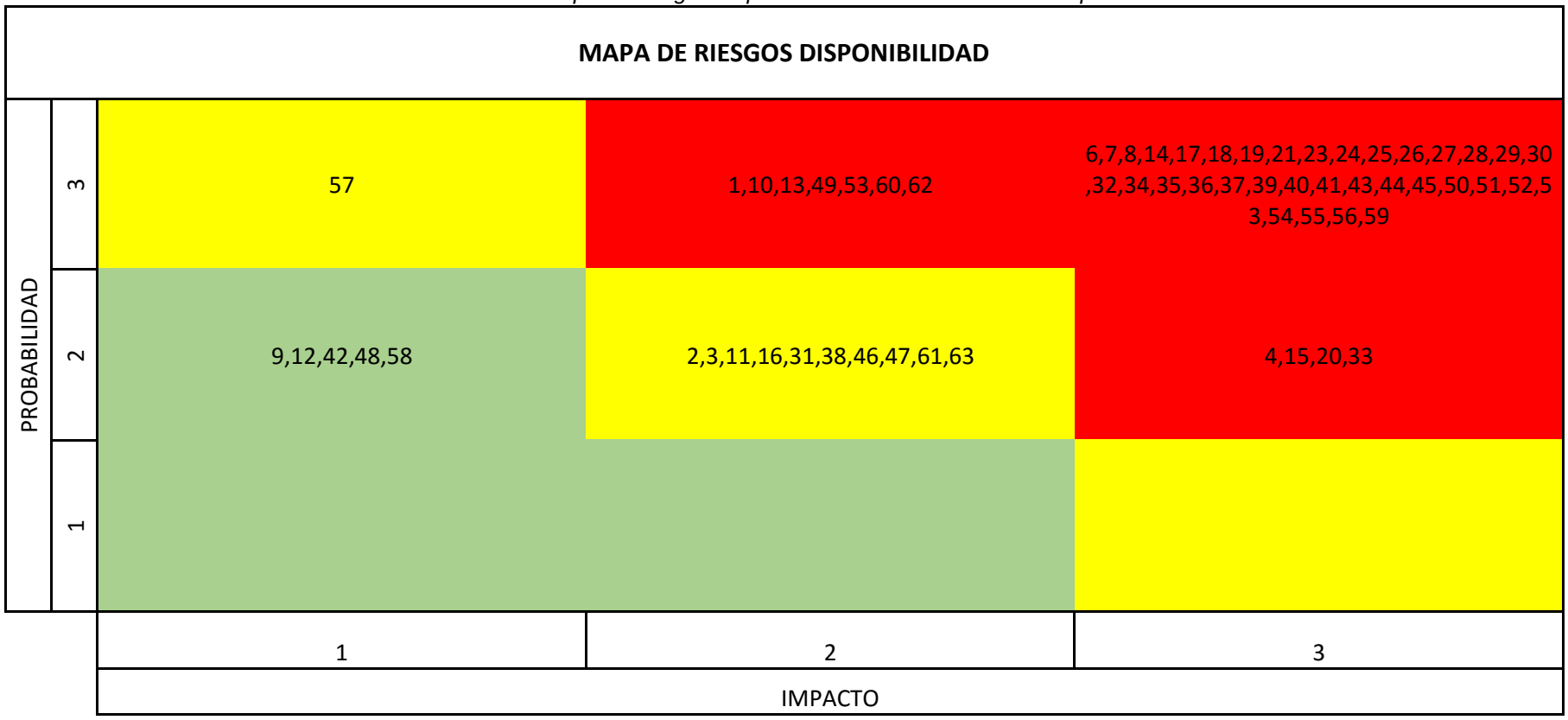
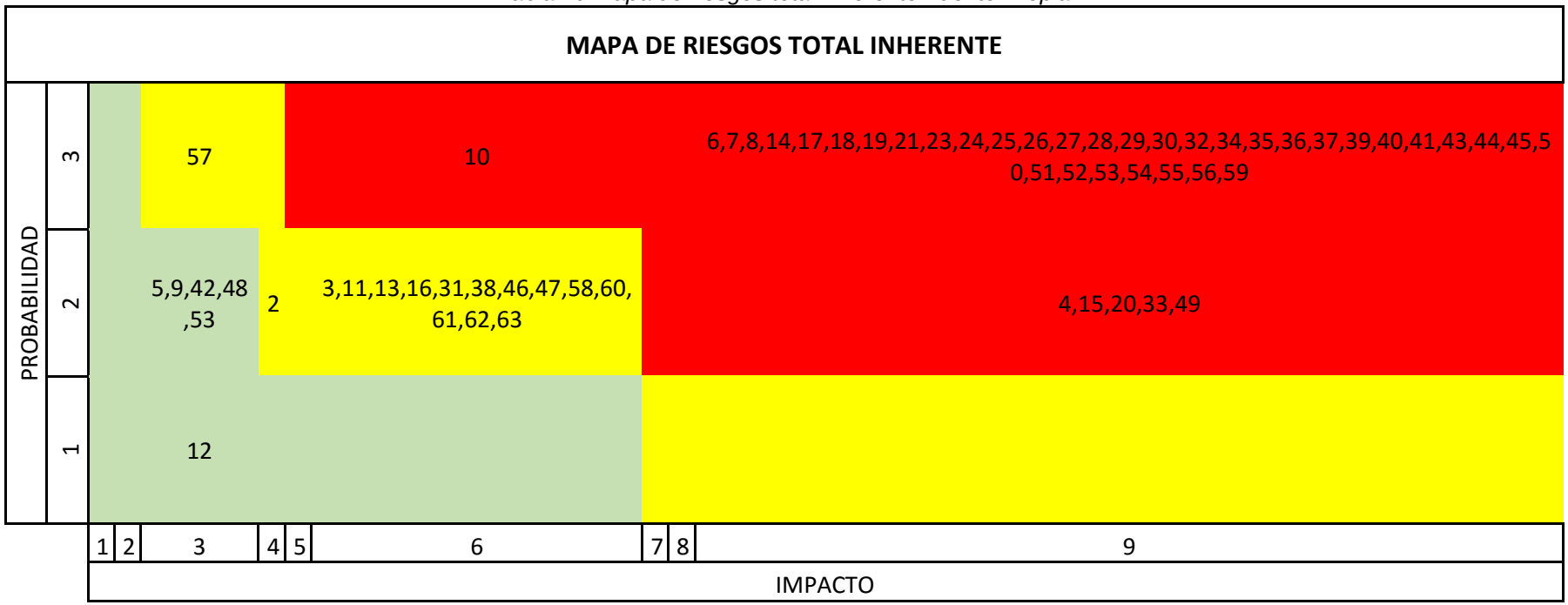


Tabla 29 Mapa de riesgos total inherente Fuente Propia



5.9 DEFINICIÓN DE CONTROLES

Tabla 30 Definición de controles Fuente Propia

CODIGO	ESCENARIO DE RIESGO	CODIGO CONTROL	CONTROL
1	Problemas legales por pérdida de información	A.5.1.1 A.5.1.2 A.6.1.1 A.6.1.2	*Políticas para la seguridad de la información *Revisión de las políticas para la seguridad de la Información *Roles y responsabilidades para la seguridad de la información *Separación de deberes
2	Falta de reacción apropiada y oportuna en la ocurrencia de un incidente	A.6.1.3	Contacto con las autoridades
3	Obsolescencia en los controles de seguridad de capacitación	A.6.1.4	Contacto con grupos de interés especial

4	La ejecución de un proyecto puede alterar la Confiabilidad, disponibilidad e integridad de los activos críticos	A.6.1.5	Seguridad de la información en la gestión de proyectos
5	Acceso a información crítica mediante el uso de dispositivos móviles	A.6.2.1	Políticas para dispositivos móviles
6	Tratamiento inadecuado de la información debido a la falta de claridad en las condiciones de trabajo	A.7.1.2 A.7.2.1	*Termino y condiciones del empleo *Responsabilidades de la dirección
7	Tratamiento inadecuado de la información crítica por desconocimiento de la políticas y procedimientos	A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información
8	No contar con un proceso debidamente documentado, que de las directrices para adelantar procesos disciplinarios en caso de violación en la seguridad de la información	A.7.2.3	Proceso disciplinario
9	Acceso de información privilegiado por parte de un empleado que ha sido promovido	A.7.3.1	Terminación o cambio de responsabilidades de empleo

10	Perdida de activos por falta de un inventario actualizado	A.8.1.1	Inventarios de activos
11	Imposibilidad en la asignación de responsabilidades en caso de pérdida o daño de activos	A.8.1.2	Propiedad de los activos
12	Uso inadecuado de los activos por parte de los propietarios de los mismos	A.8.1.3	Uso aceptable de los activos
13	Pérdida de los activos por falta de trazabilidad en préstamo.	A.8.1.4	Devolución de activos
14	Sanciones legales por tratamiento indebido de la información	A.8.2.1	Clasificación de la información
15	Imposibilidad de recuperación de la información necesario o requerida para adelantar procesos críticos de prestación del servicio	A.8.2.2	Etiquetado de la información
16	Manejo inadecuado de activos por carencia de una adecuada clasificación de la información	A.8.2.3	Manejo de activos

17	Copia no autorizada de información crítica de la organización	A.8.3.1	Gestión de medios removibles
18	Robo de medios	A.8.3.2	Disposición de los medios
19	Pérdida de la integridad y disponibilidad de información almacenada en medios, causa por un tratamiento indebido o no autorizado por parte de las personas que las custodian o de terceros	A.8.3.3	Transferencia de los medios físicos
20	Acceso de personal no autorizado a CPD	A.9.1.1	Política de control de acceso
21	Acceso de personal no autorizado a información crítica por medio de las conexiones de red	A.9.1.2	Acceso a redes y a servicios en red
22	Acceso a los activos de información con privilegios disonantes con el perfil del usuario	A.9.2.1 A.9.2.2 A.9.2.3 A.9.2.6 A.9.3.1 A.9.4.1	*Registro y cancelación del registro de usuarios *Suministro de acceso de usuarios *Gestión de derechos de acceso privilegiado *Retiro o ajuste de los derechos de acceso *Uso de la información de autenticación secreta *Restricción de acceso de información

23	Acceso de los activos de información por parte de personal no autorizado	A.9.2.4 A.9.2.5	*Gestión de información de autenticación secreta de usuarios *Revisión de los derechos de acceso de usuarios
24	Acceso a sistemas de información por deficiencias en los sistemas de autenticación	A9.4.2	Procedimiento de ingreso seguro
25	Acceso no autorizado a los sistemas de información	A.9.4.3	Sistema de gestión de contraseñas
26	Parálisis de los servicios de los sistemas de información por el uso de programas utilitarios	A.9.4.4	Uso de programas utilitarios privilegiados
27	Instalación de código no autorizado que afecte negativamente la operación de los sistemas de información	A.9.4.5	Control de acceso a códigos fuente de programas
28	Acceso a información privilegiada	A.10.1.1 A.10.1.2	*Política sobre el uso de controles criptográficos *Gestión de llaves
29	Intrusión de personas ajenas no autorizadas a las instalaciones físicas	A.11.1.1 A.11.1.2 A.11.1.3 A.11.1.6 A.11.2.1	*Perímetro de seguridad física *Controles de acceso físico *Seguridad de oficinas, recintos e instalaciones *Áreas de despachos y carga *Ubicación y protección de equipos

30	Pérdida de activos críticos causado por desastres naturales ataques maliciosos o accidentes	A.11.1.4	Protección contra amenazas externas y ambientales
31	Sanciones legales o daño en activos	A.11.1.5	Trabajo en áreas seguras
32	Daños en los equipos por fallas de fluido eléctrico	A.11.2.2	Servicio de suministros
33	*Daños en los cableados por problemas eléctricos *Interceptación del sistema de registro de estudiantes y tesorería	A.11.2.3	Seguridad de cableado
34	Fallos en la prestación de servicio de tesorería y secretaria académica por problemas en los funcionamientos de los equipos	A.11.2.4	Mantenimientos de equipos
35	Pérdida de los equipos	A.11.2.5	Retiro de activos

36	Pérdida de los equipos o daños cuando se encuentran fuera de las instalaciones	A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones
37	Pérdida de información por falta de copias de seguridad	A.11.2.7	Disposición segura o reutilización de equipos
38	Daños en los equipos	A.11.2.8	Equipos de usuario desatendido
39	Dificultad en la recuperación de información crítica	A.11.2.9	Política de escritorio limpio y pantalla limpia
40	Error en los procedimientos de registro académico por falta de información documentada que especifique las actividades relacionadas con dicho registro	A.12.1.1	Procedimientos de operación documentados
41	Pérdida de integridad de la información en el proceso de registro académico	A.12.1.2	Gestión de cambios

42	Deficiencias en la atención de la comunidad académica por recursos insuficientes	A.12.1.3	Gestión de capacidad
43	Errores de disponibilidad de la información académica y tesorería por uso de software sin haber realizado pruebas	A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación
44	Interceptación de información por código maliciosos instalado con o sin voluntad por el usuario del sistema	A.12.2.1	Controles contra códigos maliciosos
45	Perdidas de la continuidad del negocio por daños en los equipos o sistemas de información	A.12.3.1	Respaldo de la información
46	Problemas en sistemas de información sin resolver por falta de información de trazabilidad	A.12.4.1 A.12.4.3	*Registro de eventos *Registros del administrador y del operador
47	Acceso no autorizado a la información de registro	A.12.4.2	Protección de la información de registro

48	Problemas de integridad de información sin resolver por falta de sincronización de los sistemas de información	A.12.4.4	Sincronización de relojes
49	Sanciones legales por software pirata	A.12.5.1 A.12.6.2 A.12.7.1	*Instalación de software en sistemas operativos *Restricciones sobre la instalación de software *Controles de auditoria de sistemas de información
50	Acceso no autorizado a información crítica	A.12.6.1	Gestión de las vulnerabilidades técnicas
51	Acceso no autorizado a información crítica a través de las redes	A.13.1.1 A.13.1.2 A.13.1.3 A.13.2.1 A.13.2.2 A.13.2.3 A.13.2.4 A.14.1.2 A.14.1.3	*Controles de redes *Seguridad de los servicios de red *Separación en las redes *Políticas y procedimientos de transferencia de información *Acuerdos sobre transferencia de información *Mensajería electrónica *Acuerdos de confidencialidad o de no divulgación *Seguridad de servicios de las aplicaciones en redes públicas *Protección de transacciones de los servicios de las aplicaciones

52	Acceso no autorizado en los sistemas de información de secretaria académica mediante la explotación de vulnerabilidades	A.14.1.1	Análisis y especificación de requisitos de seguridad de la información
53	Fallos en la prestación del servicio por falta de pruebas	A.14.2.3 A.14.2.9	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación *Prueba de aceptación de sistemas
54	Daños en la información original comprometiendo la disponibilidad, integridad y confidencialidad de la información	A.14.3.1	Protección de datos de prueba
55	Acceso no autorizado a información crítica	A.15.1.1 A.15.1.2	*Política de seguridad de la información para las relaciones con proveedores *Tratamiento de la seguridad dentro de los acuerdos con proveedores
56	Fuga de información de los dicentes por parte de los proveedores que intervienen en los sistemas de información	A.15.1.3 A.15.2.1 A.15.2.2	*Cadena de suministro de tecnología de información y comunicación *Seguimiento y revisión de los servicios de los proveedores *Gestión de cambios en los servicios de los proveedores

57	Pérdida de imagen por no atención oportuna por daños en los activos	A.16.1.1 A.16.1.2 A.16.1.3 A.16.1.4 A.16.1.5 A.16.1.6 A.16.1.7	*Responsabilidades y procedimientos *Reportes de eventos de seguridad de información *Reporte de debilidades de seguridad de la información *Evaluación de eventos de seguridad de la información y decisiones sobre de ellos *Respuesta a incidentes de seguridad de la información *Aprendizaje obtenidos de los incidentes de seguridad de la información *Recolección de evidencia
58	No se presta el servicio de registro académico permanentemente a los usuarios a consecuencia de un desastre natural	A.17.1.1 A.17.1.2 A.17.1.3	*Planificación de la continuidad de la seguridad de la información *Implementación de la continuidad de la seguridad de la información *Verificación, revisión y evaluación de la continuidad de la seguridad de la información
59	Ausencia de información crítica redundante que garantice la disponibilidad y la continuidad de los procesos críticos (registro académico y tesorería)	A.17.2.1	Disponibilidad de instalaciones de procesamiento de información
60	Sanciones legales por uso inadecuado de la información de conformidad por lo dispuesto por el MEN	A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales

61	Sanciones legales por uso inadecuado de la información de conformidad por lo dispuesto por la legislación de derechos de autor	A.18.1.2	Derechos de propiedad intelectual
62	Sanciones legales por uso inadecuado de la información de conformidad por lo dispuesto por el MEN y la ley de habeas data	A.18.1.3 A.18.1.4 A.18.1.5	*Protección de registros *Privacidad y protección de información de datos personales *Reglamentación de controles criptográficos
63	Ausencia de controles alineados a la realidad operativa de la seguridad de la información por falta de revisiones periódicas	A.18.2.1 A.18.2.2 A.18.2.3	*Revisiones independiente de la seguridad de la información *Cumplimiento con las políticas y normas de seguridad *Revisión del cumplimiento técnico

5.10 CALIFICACIÓN DEL RIESGO RESIDUAL

Se definen los siguientes criterios para la calificación de la probabilidad

Tabla 31 Criterios para la calificación de probabilidades Fuente Propia

TABLA DE PROBABILIDADES		
VALOR	**PROBABILIDAD**	**DESCRIPCIÒN**
3	ALTO	Más de 10 veces al año o alta probabilidad de ocurrencia
2	MEDIO	Entre 5 y 10 veces al año o mediana probabilidad de ocurrencia
1	BAJO	Menos de 5 veces al año o baja probabilidad de ocurrencia

Para la calificación del impacto potencial se tomaron los criterios establecidos por la Norma NISP 800-60

Tabla 32 Criterios del Impacto potencial Fuente NIST SP 800-60 (2008)

IMPACTO POTENCIAL			
	BAJO (1)	**MODERADO (2)**	**ALTO (3)**
CONFIDENCIALIDAD La preservación de las restricciones autorizadas sobre el acceso y divulgación de información, que incluye medios para la protección de la intimidad personal y la propiedad de la información.	la divulgación no autorizada de información podría tener un efecto adverso **limitado** en las operaciones de la organización, los activos de la organización o sus individuos	se podría esperar que la divulgación no autorizada de información tenga un efecto adverso **serio** sobre las operaciones de la organización, los activos de la organización o sus individuos.	la divulgación no autorizada de información podría tener un efecto adverso **grave o catastrófico** en las operaciones de la organización, los activos de la organización, o individuos.
INTEGRIDAD Protección contra la inapropiada modificación o destrucción de información, e incluye garantizar el no repudio y la autenticidad de la información.	La modificación o destrucción no autorizada de información podrían tener un efecto adverso **limitado** en las operaciones de la organización, los activos de la organización o sus individuos	La modificación o destrucción no autorizada de información podrían tener un efecto adverso **serio** en las operaciones de la organización, los activos de la organización o sus individuos	La modificación o destrucción no autorizada de información podrían tener un efecto adverso **grave o catastrófico** en las operaciones de la organización, los activos de la organización o sus individuos

DISPONIBILIDAD Garantizar el acceso oportuno y confiable y uso de la información.	La interrupción del acceso o uso de información o a un sistema de información podría tener un efecto adverso **limitado** en las operaciones de la organización, los activos de la organización, o sus individuos.	La interrupción del acceso o uso de información o a un sistema de información podría tener un efecto adverso **serio** en las operaciones de la organización, los activos de la organización, o sus individuos.	La interrupción del acceso o uso de información o a un sistema de información podría tener un efecto adverso **grave o catastrófico** en las operaciones de la organización, los activos de la organización, o sus individuos.

Tabla 33 Escenario de riesgos Fuente Propia

CODIGO	ESCENARIO DE RIESGO	PROBABILIDAD	IMPACTO				VULNERABILIDAD RESIDUAL			
			C	I	D	TOTAL	C	I	D	T
1	Problemas legales por pérdida de información	2	2	2	2	6	44,44%	44,44%	44,44%	44,44%
2	Falta de reacción apropiada y oportuna en la ocurrencia de un incidente	2	0	0	1	1	0,00%	0,00%	2,00%	7,41%

3	Obsolescencia en los controles de seguridad por falta de capacitación	2	1	1	1	3	22,22%	22,22%	22,22%	22,22%
4	La ejecución de un proyecto puede alterar la Confiabilidad, disponibilidad e integridad de los activos críticos	1	3	3	3	9	33,33%	33,33%	33,33%	33,33%
5	Acceso a información crítica mediante el uso de dispositivos móviles	1	3	0	0	3	33,33%	0,00%	0,00%	11,11%
6	Tratamiento inadecuado de la información debido a la falta de claridad en las condiciones de trabajo	2	3	3	3	9	66,67%	66,67%	66,67%	66,67%
7	Tratamiento inadecuado de la información crítica por desconocimiento de la políticas y procedimientos	2	3	3	3	9	66,67%	66,67%	66,67%	66,67%
8	No contar con un proceso debidamente documentado, que de las directrices para adelantar procesos disciplinarios en caso de violación en la seguridad de la información	3	2	2	2	6	66,67%	66,67%	66,67%	66,67%

9	Acceso de información privilegiado por parte de un empleado que ha sido promovido	1	1	1	1	3	11,11%	11,11%	11,11%	11,11%
10	Perdida de activos por falta de un inventario actualizado	2	2	2	2	6	44,44%	44,44%	44,44%	44,44%
11	Imposibilidad en la asignación de responsabilidades en caso de pérdida o daño de activos	2	2	2	2	6	44,44%	44,44%	44,44%	44,44%
12	Uso inadecuado de los activos por parte de los propietarios de los mismos	1	1	1	1	3	11,11%	11,11%	11,11%	11,11%
13	Pérdida de los activos por falta de trazabilidad en préstamo.	3	2	2	2	6	66,67%	66,67%	66,67%	66,67%
14	Sanciones legales por tratamiento indebido de la información	2	3	3	3	9	66,67%	66,67%	66,67%	66,67%
15	Imposibilidad de recuperación de la información necesario o requerida para adelantar procesos críticos de prestación del servicio	1	2	2	2	6	22,22%	22,22%	22,22%	22,22%
16	Manejo inadecuado de activos por carencia de una adecuada clasificación de la información	1	2	2	2	6	22,22%	22,22%	22,22%	22,22%

17	Copia no autorizada de información crítica de la organización	2	3	3	3	9	66,67%	66,67%	66,67%	66,67%
18	Robo de medios	2	3	3	3	9	66,67%	66,67%	66,67%	66,67%
19	Pérdida de la integridad y disponibilidad de información almacenada en medios, causa por un tratamiento indebido o no autorizado por parte de las personas que las custodian o de terceros	2	3	3	3	9	66,67%	66,67%	66,67%	66,67%
20	Acceso de personal no autorizado a CPD	1	3	3	3	9	33,33%	33,33%	33,33%	33,33%
21	Acceso de personal no autorizado a información crítica por medio de las conexiones de red	2	3	3	3	9	66,67%	66,67%	66,67%	66,67%
22	Acceso a los activos de información con privilegios disonantes con el perfil del usuario	1	3	3	3	9	33,33%	33,33%	33,33%	33,33%
23	Acceso de los activos de información por parte de personal no autorizado	2	3	3	3	9	66,67%	66,67%	66,67%	66,67%
24	Acceso a sistemas de información por deficiencias en los sistemas de autenticación	1	3	3	3	9	33,33%	33,33%	33,33%	33,33%

25	Acceso no autorizado a los sistemas de información	1	3	3	3	9	33,33%	33,33%	33,33%	33,33%
26	Parálisis de los servicios de los sistemas de información por el uso de programas utilitarios	1	3	3	3	9	33,33%	33,33%	33,33%	33,33%
27	Instalación de código no autorizado que afecte negativamente la operación de los sistemas de información	1	3	3	3	9	33,33%	33,33%	33,33%	33,33%
28	Acceso a información privilegiada	1	3	3	3	9	33,33%	33,33%	33,33%	33,33%
29	Intrusión de personas ajenas no autorizadas a las instalaciones físicas	1	3	3	3	9	33,33%	33,33%	33,33%	33,33%
30	Pérdida de activos críticos causado por desastres naturales ataques maliciosos o accidentes	1	3	3	3	9	33,33%	33,33%	33,33%	33,33%
31	Sanciones legales o daño en activos	1	2	2	2	6	22,22%	22,22%	22,22%	22,22%
32	Daños en los equipos por fallas de fluido eléctrico	1	3	3	3	9	33,33%	33,33%	33,33%	33,33%
33	*Daños en los cableados por problemas eléctricos *Interceptación del sistema de registro de estudiantes y tesorería	1	3	3	3	9	33,33%	33,33%	33,33%	33,33%

34	Fallos en la prestación de servicio de tesorería y secretaria académica por problemas en los funcionamientos de los equipos	1	3	3	3	9	33,33%	33,33%	33,33%	33,33%
35	Pérdida de los equipos	1	3	3	3	9	33,33%	33,33%	33,33%	33,33%
36	Pérdida de los equipos o daños cuando se encuentran fuera de las instalaciones	1	3	3	3	9	33,33%	33,33%	33,33%	33,33%
37	Pérdida de información por falta de copias de seguridad	1	3	3	3	9	33,33%	33,33%	33,33%	33,33%
38	Daños en los equipos	1	2	2	2	6	22,22%	22,22%	22,22%	22,22%
39	Dificultad en la recuperación de información crítica	1	3	3	3	9	33,33%	33,33%	33,33%	33,33%
40	Error en los procedimientos de registro académico por falta de información documentada que especifique las actividades relacionadas con dicho registro	1	3	3	3	9	33,33%	33,33%	33,33%	33,33%
41	Pérdida de integridad de la información en el proceso de registro académico	1	3	3	3	9	33,33%	33,33%	33,33%	33,33%
42	Deficiencias en la atención de la comunidad académica por recursos insuficientes	1	1	1	1	3	11,11%	11,11%	11,11%	11,11%

43	Errores de disponibilidad de la información académica y tesorería por uso de software sin haber realizado pruebas	3	1	1	1	3	33,33%	33,33%	33,33%	33,33%
44	Interceptación de información por código maliciosos instalado con o sin voluntad por el usuario del sistema	1	3	3	3	9	33,33%	33,33%	33,33%	33,33%
45	Perdidas de la continuidad del negocio por daños en los equipos o sistemas de información	3	1	1	1	3	33,33%	33,33%	33,33%	33,33%
46	Problemas en sistemas de información sin resolver por falta de información de trazabilidad	1	2	2	2	6	22,22%	22,22%	22,22%	22,22%
47	Acceso no autorizado a la información de registro	1	3	3	3	9	33,33%	33,33%	33,33%	33,33%
48	Problemas de integridad de información sin resolver por falta de sincronización de los sistemas de información	1	1	1	1	3	11,11%	11,11%	11,11%	11,11%
49	Sanciones legales por software pirata	1	2	2	2	6	22,22%	22,22%	22,22%	22,22%
50	Acceso no autorizado a información crítica	1	3	3	3	9	33,33%	33,33%	33,33%	33,33%
51	Acceso no autorizado a información crítica a través de las redes	1	3	3	3	9	33,33%	33,33%	33,33%	33,33%

52	Acceso no autorizado en los sistemas de información de secretaria académica mediante la explotación de vulnerabilidades	1	3	3	3	9	33,33%	33,33%	33,33%	33,33%
53	Fallos en la prestación del servicio por falta de pruebas	1	1	0	0	1	11,11%	0,00%	0,00%	3,70%
54	Daños en la información original comprometiendo la disponibilidad, integridad y confidencialidad de la información	1	3	3	3	9	33,33%	33,33%	33,33%	33,33%
55	Acceso no autorizado a información crítica	1	3	3	3	9	33,33%	33,33%	33,33%	33,33%
56	Fuga de información de los dicentes por parte de los proveedores que intervienen en los sistemas de información	1	3	3	3	9	33,33%	33,33%	33,33%	33,33%
57	Pérdida de imagen por no atención oportuna por daños en los activos	1	1	1	1	3	11,11%	11,11%	11,11%	11,11%
58	No se presta el servicio de registro académico permanentemente a los usuarios a consecuencia de un desastre natural	2	1	1	1	3	22,22%	22,22%	22,22%	22,22%
59	Ausencia de información crítica redundante que garantice la disponibilidad y la continuidad de	1	3	3	3	9	33,33%	33,33%	33,33%	33,33%

	los procesos críticos (registro académico y tesorería)									
60	Sanciones legales por uso inadecuado de la información de conformidad por lo dispuesto por el MEN	1	2	2	2	6	22,22%	22,22%	22,22%	22,22%
61	Sanciones legales por uso inadecuado de la información de conformidad por lo dispuesto por la legislación de derechos de autor	1	2	2	2	6	22,22%	22,22%	22,22%	22,22%
62	Sanciones legales por uso inadecuado de la información de conformidad por lo dispuesto por el MEN y la ley de habeas data	1	2	2	2	6	22,22%	22,22%	22,22%	22,22%
63	Ausencia de controles alineados a la realidad operativa de la seguridad de la información por falta de revisiones periódicas	1	2	2	2	6	22,22%	22,22%	22,22%	22,22%

5.11 MAPA DE RIESGOS RESIDUAL

Tabla 34 Criterios de aceptabilidad del riesgo residual Fuente Propia

CRITERIOS DE ACEPTABILIDAD DEL RIESGO

IDENTIFICACIÓN	CRITERIO	DESCRIPCIÓN
	ACEPTABLE	Vulnerabilidad < 25%
	TOLERABLE	Vulnerabilidad entre el 25 y el 50%
	INACEPTABLE	Vulnerabilidad superior al 50%

Tabla 35 Mapa de riesgos confidencialidad residual Fuente Propia

MAPA DE RIESGOS CONFIDENCIALIDAD				
PROBABILIDAD	3	43	13	8,24,50
	2	3,58	1,10,	6,7,17,18,19,3
	1	9,12,42,48,53,57	15,16,31,38,46,60,61,62,63	4,5,20,23,25,26,27,28,29,30,32,33,34,35,36, 37,39,40,41,44,45,47,51,52,54,55,56,59
		1	2	3
		IMPACTO		

Tabla 36 Mapa de riesgo integridad residual Fuente Propia

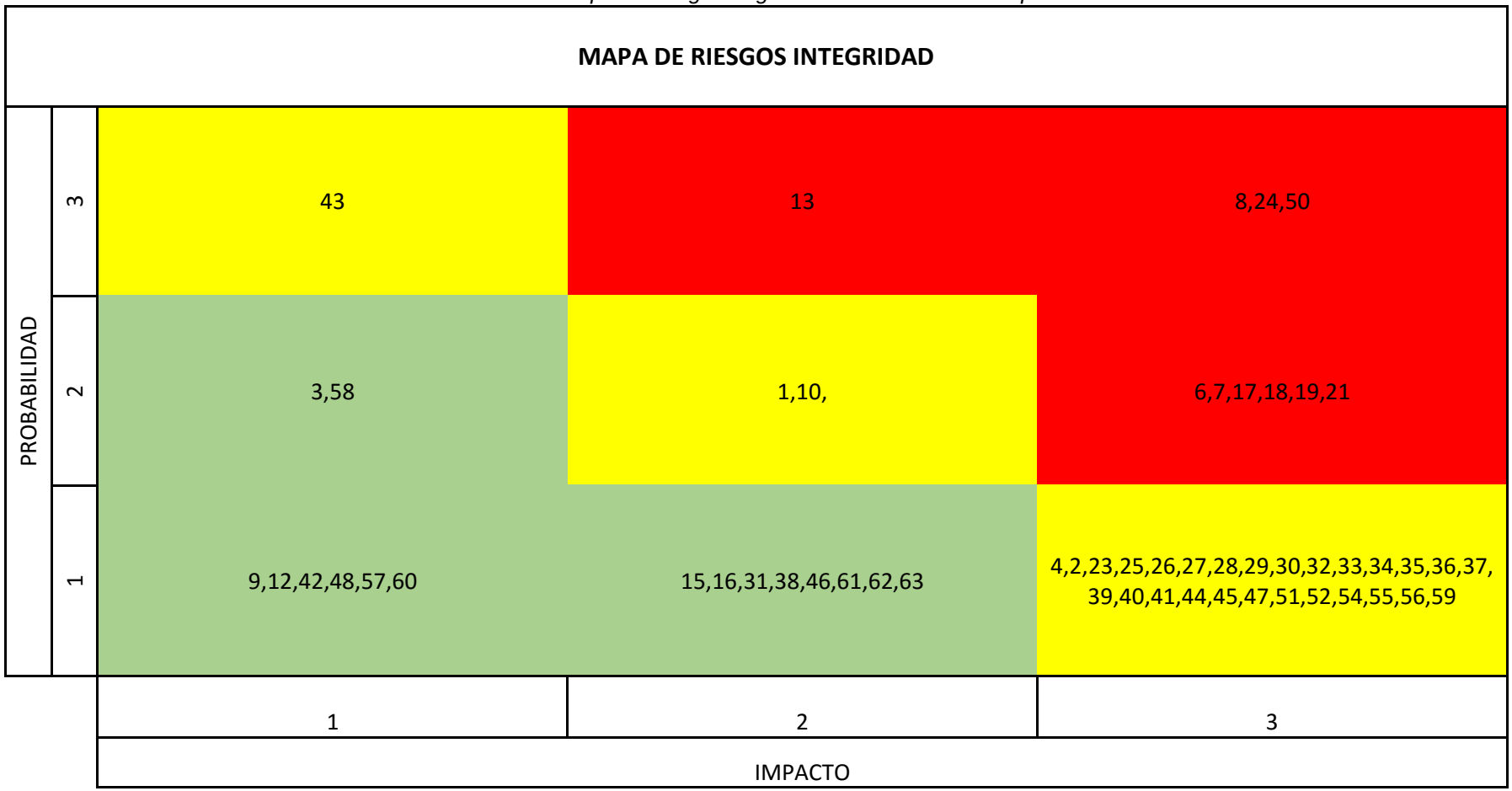


Tabla 37 Mapa de riesgo disponibilidad residual Fuente Propia

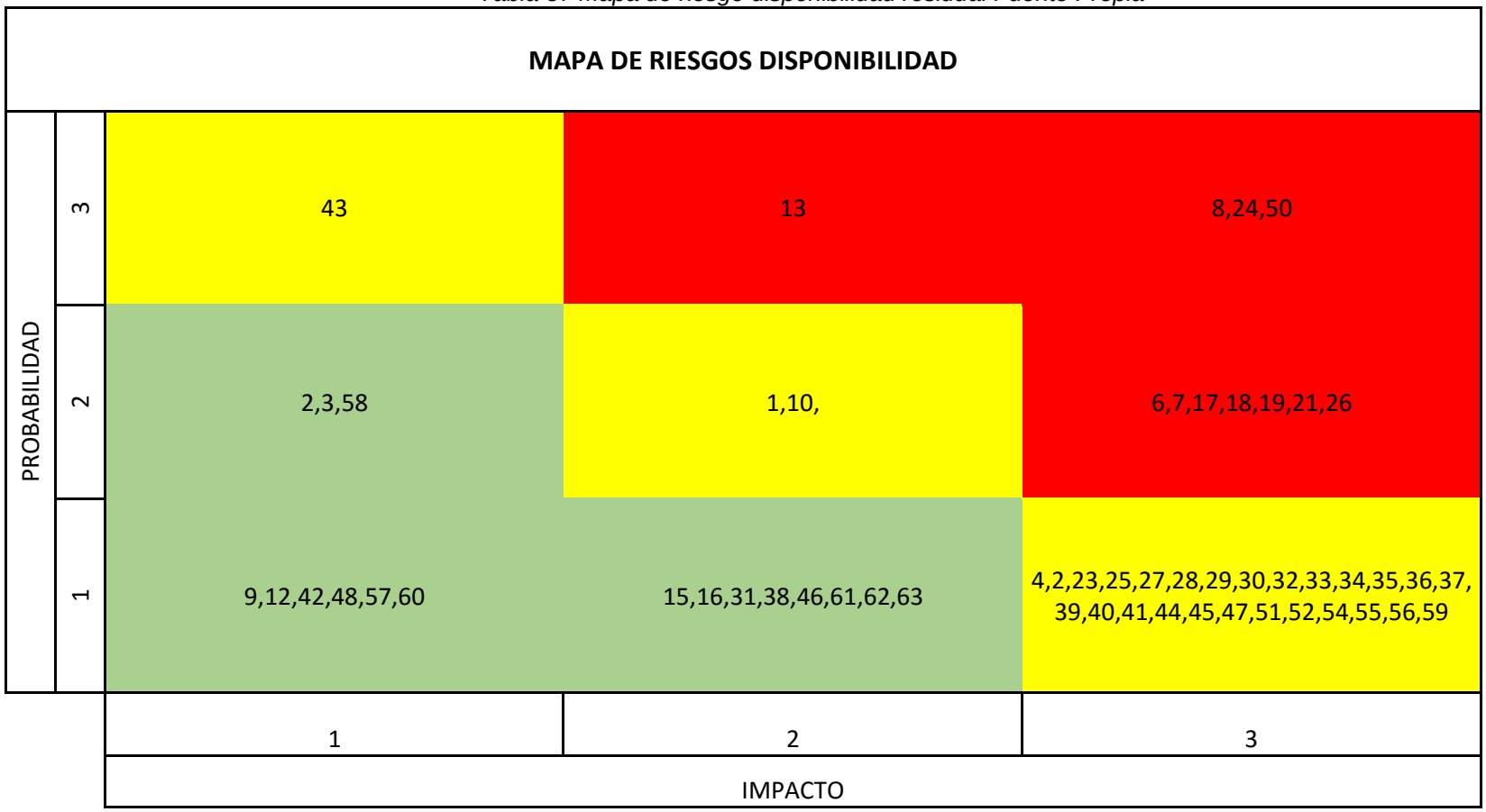
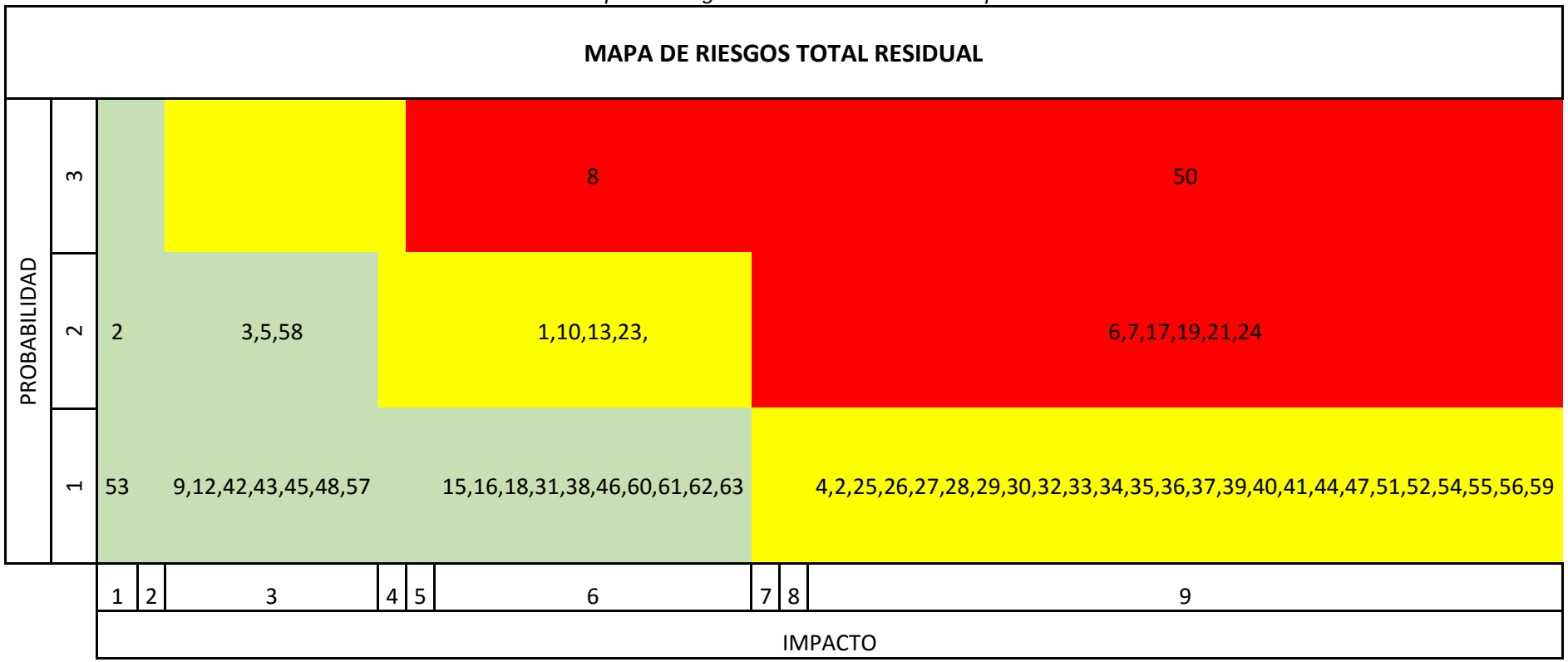


Tabla 38 Mapa de riesgos total residual Fuente Propia



5.12 PLAN DE MITIGACIÓN DE RIESGOS

Tabla 39 Plan de mitigación de riesgos Fuente Propia

CODIGO	ESCENARIO DE RIESGO	PLAN DE MITIGACIÓN DE RIESGOS		
		ACTIVIDAD	RESPONSABLE	COSTO
1	Problemas legales por pérdida de información	*Se requiere establecer las políticas necesarias que definan los lineamientos internos para asegurar los activos de información critico que contienen información confidencial o son vitales para la continuidad de las operaciones de la institución *Definir revisiones periódicas a las políticas de seguridad para asegurar el cumplimiento de las modificación o nuevas normas legales que involucren a la institución, así como los cambios internos que pueda sufrir la institución *La institución debe establecer las responsabilidades y roles necesarios tanto en el equipo de seguridad así como para los trabajadores internos *Es importante establecer las limitaciones de acceso en cuanto a la información crítica.	Secretaria, Coordinación académica y tesorería	Medio

2	Falta de reacción apropiada y oportuna en la ocurrencia de un incidente	La institución debe establecer el procedimiento a seguir para la notificación de un incidente de seguridad de la información, así como la identificación de las autoridades pertinentes - policía, entes reguladores, etc, permitirá que dichos eventos no pasen desapercibidos, recibiendo el tratamiento adecuado por parte de las autoridades correspondientes	Seguridad	Bajo
3	Obsolescencia en los controles de seguridad de capacitación	La institución debe establecer comunicación con los grupos de interés a los que pertenece en este caso, al núcleo, las secretarias de educación, ministerio de educación nacional	Rectoría	Bajo
4	La ejecución de un proyecto puede alterar la Confiabilidad, disponibilidad e integridad de los activos críticos	Los proyectos que se realicen dentro del alcance del presente proyecto deberán ser gestionado debidamente mediante una metodología teniendo en cuenta la gestión de riesgos y además contar con lineamiento de seguridad de la información.	Coordinación académica y rectoría	Medio
5	Acceso a información crítica mediante el uso de dispositivos móviles	Establecer una política sobre el uso de dispositivos móviles en las áreas de información crítica	Académico	Alto

6	Tratamiento inadecuado de la información debido a la falta de claridad en las condiciones de trabajo	*Establecer procedimientos documentados que garanticen la adecuada verificación de antecedentes y cualificación de las personas que aspiran a realizar trabajos dentro de la institución *Se debe especificar la responsabilidad de la rectoría en cuanto a la implementación y el mantenimiento del SGSI puesto que hace parte del plan estratégico y a los intereses de sus estudiantes	Rectoría y secretaría	Bajo
7	Tratamiento inadecuado de la información crítica por desconocimiento de la políticas y procedimientos	Establecer un plan de capacitación de los colaboradores sobre la política de seguridad de la información, así como su evaluación permitirá medir el nivel de conocimiento de los mismo en este tema	Coordinación Académica	Medio
8	No contar con un proceso debidamente documentado, que de las directrices para adelantar procesos disciplinarios en caso de violación en la seguridad de la información	Se debe establecer la penalización disciplinaria que se debe aplicar en caso de infringir las condiciones en cuanto a la seguridad de la información con la que se trabaja	Coordinación Académica	Medio
9	Acceso de información privilegiado por parte de un empleado que ha sido promovido	Se debe establecer términos y condiciones en el momento de la incorporación, permitiendo a la institución protegerse legalmente frente a filtraciones realizadas por trabajadores cesados o promovidos	Secretaria, Coordinación académica y tesorería	Alto

10	Perdida de activos por falta de un inventario actualizado	La institución debe manejar un inventario de activos en el que se identifique el tipo de activo y su ubicación.	Área de Sistemas	Alto
11	Imposibilidad en la asignación de responsabilidades en caso de pérdida o daño de activos	Los activos de información deben ser asignados a un custodio encargado del inventario, clasificación y protección de los activos, así como de la destrucción en caso de que sea necesario, además de la revisión de las restricciones en cuanto a accesos	Área de Sistemas	Alto
12	Uso inadecuado de los activos por parte de los propietarios de los mismos	Especificar y documentar a qué se define como uso aceptable en cuanto a manejo de información personal y sensible mediante una política o procedimiento que debe ser de conocimiento obligatorio para el personal del área	Área de Sistemas	Alto
13	Pérdida de los activos por falta de trazabilidad en préstamo.	Se debe establecer un procedimiento de asignación y devolución de los activos de información, asignado o entregado al personal de la organización	Área de Sistemas	Alto
14	Sanciones legales por tratamiento indebido de la información	Realizar una clasificación de los activos identificados según su criticidad para la institución o el nivel de confidencialidad que se le debe otorgar.	Área de Sistemas	Alto

15	Imposibilidad de recuperación de la información necesario o requerida para adelantar procesos críticos de prestación del servicio	Realizar el etiquetado que identifique la información según la clasificación previamente definida, en el caso de los sistemas información los usuarios deberán ver un mensaje visible que indique la clasificación de la información al que accede.	Área de Sistemas	Alto
16	Manejo inadecuado de activos por carencia de una adecuada clasificación de la información	Establecer procedimientos de manejo de activos de información permitirá que se sigan protocolos que garanticen la seguridad de los mismo.	Área de Sistemas	Alto
17	Copia no autorizada de información crítica de la organización	Establecer procedimientos para gestión de medios removibles	Área de Sistemas y Rectoría	Alto
18	Robo de medios	Establecer un protocolo de eliminación de medios que contengan información confidencial, de manera que no pueda ser reutilizado o extraído por personas no autorizadas	Seguridad	Alto
19	Pérdida de la integridad y disponibilidad de información almacenada en medios, causa por un tratamiento indebido o no autorizado por parte de las personas que las custodian o de terceros	Se debe establecer protocolos que aseguren la información en sus transferencias físicas de manera que se garantice su integridad, y que no sea manipulada por personal no autorizado en el momento de salir e ingresar a otro sitio	Área de Sistemas, Secretaría y Rectoría	Alto
20	Acceso de personal no autorizado a CPD	Se debe establecer unas políticas donde se documente el acceso a la institución, llevando un control de ingreso y acceso a las áreas críticas	Área de Sistemas y Rectoría	Medio

21	Acceso de personal no autorizado a información crítica por medio de las conexiones de red	Establecer una política de acceso a nivel de red que establezca los lineamientos en cuanto a segmentación de redes, acceso de externos a la red interna, monitoreo, etc	Área de Sistemas	Medio

22	Acceso a los activos de información con privilegios disonantes con el perfil del usuario	*Para mitigar el riesgo de acceso no autorizado, se debe mantener un procedimiento de alta y sobretodo bajas de usuario de los sistemas de la institución *implementar un proceso de acceso con privilegios a los empleados autorizados, y que permita también retirar ese privilegio en caso de que ya sea necesario *Establecer un proceso de suministro de acceso según las funciones o áreas a las cuales cada empleado pertenece *Los privilegios con los que cuentan los empleados deberán ser eliminados en el caso en que el trabajador, haya cesado su relación con la Institución, o ajustados a lo largo del tiempo en caso en el que el empleado requiera mayores privilegios o ya no los necesita Se debe establecer el uso de los métodos de autenticación, así como los requisitos para asegurar la confidencialidad de estos datos. *Establecer un doble control de autenticación en aquellos sistemas en los que se encuentra información sensible	Área de Sistemas	Alto

23	Acceso de los activos de información por parte de personal no autorizado	*Se debe establecer las directivas de uso de los métodos de autenticación, así como los requisitos para asegurar la confidencialidad de estos datos siento indispensable que estas directivas, se hagan publica a todos los empleados de la institución *Los responsables de los activos de información son quienes deben vigilar que empleados puede acceder a los activos de información, además de revisar periódicamente los usuarios que tienen permiso para identificar los que ya no están autorizados a acceder	Área de Sistemas	Medio
24	Acceso a sistemas de información por deficiencias en los sistemas de autenticación	Establecer un doble control de autenticación en aquellos sistemas en los que se encuentra información sensible	Área de Sistemas	Medio
25	Acceso no autorizado a los sistemas de información	Establecer un control enfocado a proteger la información de inicio de sesión del usuario en los sistemas de forma que no pueda ser sustraída por un agente externo	Académico	Alto

26	Parálisis de los servicios de los sistemas de información por el uso de programas utilitarios	Establecer requisitos mínimos en cuanto a complejidad de contraseñas, los procedimientos de cambios de contraseñas y el almacenamiento de las mismas entre otros	Área de Sistemas	Alto
27	Instalación de código no autorizado que afecte negativamente la operación de los sistemas de información	Identificar los lineamientos de uso de utilidades ya sean internas o externas, traídas por los empleados a la Institución	Área de Sistemas	Bajo
28	Acceso a información privilegiada	Implementar controles y políticas sobre el manejo criptográficos para garantizar la protección de la información	Área de Sistemas	Alto

29	Intrusión de personas ajenas no autorizadas a las instalaciones físicas	*Establecer un límite de acceso físico a los empleados y personal externo a las áreas donde se encuentran la información crítica *Utilizar controles de registro de acceso para el personal que requiera ingresar a los ambientes donde se almacena la información crítica, debe está debidamente identificado en todo momento Se debe evitar el acceso de personal no autorizado o al público que hace uso de los servicios de la Institución a los ambientes en los que se almacena información sensible *Establecer puntos alejados de las áreas críticas, donde se permita cargar y descargar elementos para la institución, Los equipos deben instalarse de manera que se evite el acceso no autorizado a los mismo por parte de personas ajenas al servicio	Seguridad	Medio

30	Pérdida de activos críticos causado por desastres naturales ataques maliciosos o accidentes	Implementar medidas para proteger la información crítica frente a incidentes que puedan afectar tanto naturales como provocados como los incendios	Comité	Alto
31	Sanciones legales o daño en activos	Establecer puntos alejados de las áreas críticas, donde se permita trabajar de forma segura	Jefe de sistemas y Rectoría	Alto
32	Daños en los equipos por fallas de fluido eléctrico	Los equipos críticos relacionados al manejo de información sensible deben contar con medidas que aseguran su funcionamiento en el caso de caída de algún servicio como el fluido eléctrico	Comité	Alto
33	*Daños en los cableados por problemas eléctricos *Interceptación del sistema de registro de estudiantes y tesorería	Adecuar el cableado estructurado, de tal forma que no sea posible intervenir o dañar, interrumpiendo el servicio, o extraer información	Área de Sistemas y Rectoría	Alto
34	Fallos en la prestación de servicio de tesorería y secretaria académica por problemas en los funcionamientos de los equipos	Los equipos que cuentan con acceso a información crítica deberán seguir un procedimiento de mantenimiento adecuado, de manera que la información que contiene sea comprometida	Área de Sistemas y Rectoría	Alto
35	Pérdida de los equipos	La institución debe establecer políticas que limiten el retiro de la información sensible de las instalaciones a excepción de ser para cumplir con alguno de los servicios que brinda	Área de Sistemas y Rectoría	Alto

36	Pérdida de los equipos o daños cuando se encuentran fuera de la instaciones	La institución debe asegurar que el uso de la información crítica de la institución que maneja haya sido autorizado por las personas correspondientes	Área de Sistemas y Rectoría	Alto
37	Pérdida de información por falta de copias de seguridad	Los equipos que se den de baja o se cambien de área deben hacer pasado por un proceso de limpieza que garantice la eliminación completa de toda la información sensible que pueda contener	Área de Sistemas y Rectoría	Alto
38	Daños en los equipos	Los empleados deberán mantener la seguridad de sus equipos incluso cuando se levantan del puesto de trabajo para dirigirse a otro sector, o cuando no se está trabajando	Área de Sistemas	Alto
39	Dificultad en la recuperación de información crítica	Los empleados deberán mantener los escritorios libres de cualquier información crítica que pueda ser usada o extraída por persona externo.	Área de Sistemas	Medio
40	Error en los procedimientos de registro académico por falta de información documentada que especifique las actividades relacionadas con dicho registro	Se requiere la documentación de los procesos que se tienen en la institución con el fin de determinar el área más crítica, y realizar una evaluación continua sobre el nivel de riesgo existente, para establecer controles necesarios	Área de Sistemas, secretaría y Coordinación académica	Alto
41	Pérdida de integridad de la información en el proceso de registro académico	Se deben controlar los cambios en la institución y en los sistemas de procesamiento de información, que afecte la seguridad de la información.	Área de Sistemas, Rectoría y Coordinación académica	Alto

42	Deficiencias en la atención de la comunidad académica por recursos insuficientes	Se debe hacer seguimiento al uso de recursos y establecer si se necesita más recursos para asegurar el desempeño requerido del sistema.	Rectoría	Alto
43	Errores de disponibilidad de la información académica y tesorería por uso de software sin haber realizado pruebas	Se deben separar las áreas, para reducir los riesgos de acceso o cambios no autorizados el área donde se encuentre información crítica	Área de Sistemas	Medio
44	Interceptación de información por código maliciosos instalado con o sin voluntad por el usuario del sistema	debido al gran avance de amenazas informáticas, la institución deberá asegurar que los equipos de cómputo se encuentren debidamente protegidos ante software malicioso que ponga en peligro la información sensible de la institución	Área de Sistemas	Medio
45	Perdidas de la continuidad del negocio por daños en los equipos o sistemas de información	Establecer una política de respaldo que garantice la continuidad de la atención y mitigue la pérdida de datos en caso de incidente	Área de Sistemas	Alto

46	Problemas en sistemas de información sin resolver por falta de información de trazabilidad	*Establecer una política de respaldo que garantice la continuidad de la atención y mitigue la pérdida de datos en caso de incidente *Los usuarios que accedan a información crítica deben contar con un login y contraseña con el fin de que se genere un registro de los movimientos realizados por cada usuario	Académico	Alto
47	Acceso no autorizado a la información de registro	Los usuarios que accedan a información crítica deben contar con un login y contraseña con el fin de que se genere un registro de los movimientos realizados por cada usuario	Área de Sistemas	Alto
48	Problemas de integridad de información sin resolver por falta de sincronización de los sistemas de información	Realizar una revisión a los equipos para garantizar que estén ajustados a la hora establecida en el país	Área de Sistemas	Alto

49	Sanciones legales por software pirata	*Realizar auditorías periódicas a los equipos informáticos con el fin de identificar software piratas instalados, o que no son permitidos en la institución *Establecer una política que evite que el personal pueda instalar aplicaciones no licenciadas o no permitidas, también se puede restringir las cuentas para que no permita instalar programas *Se debe realizar una auditoría periódica de modo que se verifique el buen funcionamiento y uso de los sistemas de información además de asegurar que solo los usuarios debidamente autorizados cuenten con acceso a la información sensible	Área de Sistemas	Alto
50	Acceso no autorizado a información crítica	Se debe establecer una política de revisión periódica para analizar las vulnerabilidades en los equipos donde se almacena información crítica.	Área de Sistemas	Alto

51	Acceso no autorizado a información crítica a través de las redes	*La red interna de la institución debe contar con los controles necesarios para asegurar que la información viaje a través de la misma, de modo que no puede ser capturada por un agente externo al flujo de información *Se debe contar con un inventario de servicios de red que establezca los niveles de servicio que deben cumplir además de las características de seguridad con lo que se cuenta *Se deben contar con una correcta separación tanto de redes, como de usuarios en el dominio de la institución que permita verificar los accesos brindados y puedan ser verificados *Se deben contar con una correcta separación tanto de redes, como de usuarios en el dominio de la institución que permita verificar los accesos brindados y puedan ser verificados *Durante la transferencia de información se debe especificar a la entidad que la recibe la categoría de la información si es sensible, confidencial o	Área de Sistemas	Alto

		crítica, e indicar mediante un acuerdo de condiciones la confidencialidad de la misma La institución debe establecer acuerdos de confidencialidad que detallen las limitaciones de divulgación de la información por sus empleados *La red interna de la institución debe contar con los controles necesarios para asegurar que la información viaje a través de la misma, de modo que no puede ser capturada por un agente externo al flujo de información La red interna de la institución debe contar con los controles necesarios para asegurar que la información viaje a través de la misma, de modo que no puede ser capturada por un agente externo al flujo de información		

52	Acceso no autorizado en los sistemas de información de secretaria académica mediante la explotación de vulnerabilidades	La red interna de la institución debe contar con los controles necesarios para asegurar que la información viaje a través de la misma, de modo que no puede ser capturada por un agente externo al flujo de información	Área de Sistemas	Alto
53	Fallos en la prestación del servicio por falta de pruebas	*Se debe solicitar pruebas que garantice que al realizar cambios de *software para operaciones en la institución, no se generen pérdidas o daños a la información, además de realizar una copia de seguridad previa *Se debe solicitar pruebas que garantice que, al realizar cambios de software para operaciones en la institución, no se generen pérdidas o daños a la información, además de realizar una copia de seguridad previa	Área de Sistemas	Alto
54	Daños en la información original comprometiendo la disponibilidad, integridad y confidencialidad de la información	Se debe solicitar pruebas que garantice que, al realizar cambios de software para operaciones en la institución, no se generen pérdidas o daños a la información, además de realizar una copia de seguridad previa	Área de Sistemas	Alto

55	Acceso no autorizado a información crítica	*Documentar todos los procesos realizados por los proveedores externos Documentar todos los procesos realizados por los proveedores externos	Área de Sistemas	Alto
56	Fuga de información de los dicentes por parte de los proveedores que intervienen en los sistemas de información	*Realizar auditoria a los servicios prestados por los proveedores de la institución *Se debe establecer una política de auditoria permanente a los proveedores de la institución *Realizar auditoria a los servicios prestados por los proveedores de la institución	Académico	Alto

57	Pérdida de imagen por no atención oportuna por daños en los activos	*Se debe detallar las responsabilidades y procedimientos correspondientes a dicho equipo de manera que se encuentren debidamente identificadas las funciones del mismo *Realizar revisiones para identificar eventos o vulnerabilidades y deben ser reportados para su análisis *Analizar los eventos encontrados por el equipo, determinando las acciones para evitar incidentes *Se debe documentar y dejar historial de todo los eventos que se identifiquen en una bitácora, con el fin de ayudar a disminuir ocurrencias futuras *Se debe recolectar todas la evidencias de los incidentes presentados.	Académico	Alto

58	No se presta el servicio de registro académico permanentemente a los usuarios a consecuencia de un desastre natural	*La institución deberá identificar los activos de información que son críticos para asegurar la continuidad de las operaciones de la institución, según el impacto de disponibilidad del servicio que tendría una pérdida de dicha información *Establecer que los planes de contingencia la protección de los activos de información previamente identificados, de manera que se asegure la disponibilidad de los mismo haciendo más eficiente la recuperación de los servicios de la institución *Establecer la realización de pruebas periódicas para verificar que los planes de contingencia establecidos, así como el nivel de protección de la información esté disponible frente a los distintos escenarios que haya presentado.	Académico	Alto
59	Ausencia de información crítica redundante que garantice la disponibilidad y la continuidad de los procesos críticos (registro académico y tesorería)	La institución debe establecer servidores que almacene la información sensible o crítica para las operaciones, además deberán contar con instalaciones alternas en las cuales se almacene la información de manera redundante, con el fin de recuperar la información en caso de una emergencia	Coordinación Académica y rectoría	Medio

60	Sanciones legales por uso inadecuado de la información de conformidad por lo dispuesto por el MEN	La institución debe contar con documentación alusivos a la normativa relacionada a seguridad de la información que afecta a la institución	Coordinación Académica y Rectoría	Alto
61	Sanciones legales por uso inadecuado de la información de conformidad por lo dispuesto por la legislación de derechos de autor	implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados	Coordinación Académico	Medio
62	Sanciones legales por uso inadecuado de la información de conformidad por lo dispuesto por el MEN y la ley de habeas data	*La institución debe contar con procedimiento que determinen las condiciones de almacenamiento de información física, el periodo de tiempo por el cual dicha información debe ser almacenada y los procedimientos estándar de desecho de información *La institución debe garantizar que la información personal de la población deberá ser protegida de acuerdo a lo indicado por la Ley de protección de datos personales *Se debe establecer controles para el uso de criptografía en cumplimiento de todos los acuerdos y reglamentación.	Coordinación Académico	Alto

63	Ausencia de controles alineados a la realidad operativa de la seguridad de la información por falta de revisiones periódicas	El sistema de Gestión de Seguridad de la información deberá ser revisado periódicamente teniendo en cuenta los cambios organizacionales o legislativos que se produzcan *Las políticas de Seguridad de la Información deberán ser evaluadas periódicamente en cuanto a su cumplimiento en la institución, así como ajustados de acuerdo a los cambios que se puedan hacer producido en el marco legal u organizacional *Los sistemas de información utilizados deben ser evaluados periódicamente en cuanto al cumplimiento de los aspectos técnicos relacionados con las políticas de seguridad de modo que se puedan detectar fallas o vulnerabilidades nuevas.	Coordinación Académico	Medio

5.13 DECLARACIÓN DE APLICABILIDAD

Tabla 40 Controles de declaración de aplicabilidad Fuente Propia

DOMINIOS	**14**
OBJETIVOS DE CONTROL	**35**
CONTROLES	**114**

Tabla 41 Políticas de la seguridad de la información Fuente Propia

A.5	Políticas de la Seguridad de la Información								
COD	**TITULO CONTROL**	**DESCRIPCIÓN OBJETIVO DE CONTROL**	**COD**	**CONTROLES**	**DESCRIPCION DEL CONTROL**	**Aplica Si/No**	**RIESGO**	**ACTIVIDAD**	**OBSERVACIONES**
A.5.1	**Orientación de la dirección para la gestión de la seguridad de la información**	**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**	A.5.1.1	Políticas para la seguridad de la información	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	SI	Problemas legales por pérdida de información	Se requiere establecer las políticas necesarias que definan los lineamientos internos para asegurar los activos de información critico que contienen información confidencial o son vitales para la continuidad de las operaciones de la institución	

			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 continúas.	Si	Problemas legales por pérdida de información	Definir revisiones periódicas a las políticas de seguridad para asegurar el cumplimiento de las modificación o nuevas normas legales que involucren a la institución, así como los cambios internos que pueda sufrir la institución	
A.6	**Organización de la seguridad de la información**								
COD	**TITULO CONTROL**	**DESCRIPCIÓN OBJETIVO DE CONTROL**	**COD**	**CONTROLES**	**DESCRIPCION DEL CONTROL**	**Aplica Si/No**	**Riesgo**	**ACTIVIDAD**	**OBSERVACIONES**
A.6.1	**Organización Interna**	**Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información**	A.6.1.1	Roles y responsabilidades para la seguridad de la información	Se deben definir y asignar todas las responsabilidades de la seguridad de la información	SI	Problemas legales por pérdida de información	La institución debe establecer las responsabilidades y roles necesarios tanto en el equipo de seguridad, así como para los trabajadores internos	

		dentro de la organización	A.6.1.2	Separación de deberes	Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	SI	Problemas legales por pérdida de información	Es importante establecer las limitaciones de acceso en cuanto a la información crítica.	
			A.6.1.3	Contacto con las autoridades	Se deben mantener contactos apropiados con las autoridades pertinentes	SI	Falta de reacción apropiada y oportuna en la ocurrencia de un incidente	La institución debe establecer el procedimiento a seguir para la notificación de un incidente de seguridad de la información, así como la identificación de las autoridades pertinentes - policía, entes reguladores, etc, permitirá que dichos eventos no pasen desapercibidos, recibiendo el tratamiento adecuado por parte de las	

								autoridades correspondientes	
			A.6.1.4	Contacto con grupos de interés especial	Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	SI	Obsolescencia en los controles de seguridad de capacitación	La institución debe establecer comunicación con los grupos de interés a los que pertenece en este caso, al núcleo, las secretarias de educación, ministerio de educación nacional	
			A.6.1.5	Seguridad de la información en la gestión de proyectos	La seguridad de la información se debe tratar en la gestión de proyectos, independientement e del tipo de proyecto.	SI	La ejecución de un proyecto puede alterar la Confiabilidad, disponibilidad e integridad de los activos críticos	Los proyectos que se realicen dentro del alcance del presente proyecto deberán ser gestionado debidamente mediante una metodología teniendo en cuenta la gestión de riesgos y además contar con lineamiento	

								de seguridad de la información.	
A6.2	**Dispositivos móviles y teletrabajo**	**Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles**	A.6.2.1	Políticas 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	SI	Acceso a información crítica mediante el uso de dispositivos móviles	Establecer una política sobre el uso de dispositivos móviles en las áreas de información crítica	
			A.6.2.2	Teletrabajo	Se deben implementar una política y unas medidas de seguridad de soporte para proteger la información a la que se tiene acceso que es procesada o almacenada en los lugares en los que se realiza teletrabajo	NO			No se considera dado a que en las instituciones educativas no se brinda el servicio de teletrabajo

A.7	Seguridad de los recursos humanos								
COD	**TITULO CONTROL**	**DESCRIPCIÓN OBJETIVO DE CONTROL**	**COD**	**CONTROLES**	**DESCRIPCION DEL CONTROL**	**Aplica Si/No**	**Riesgo**	**ACTIVIDAD**	**OBSERVACIONES**
A.7.1	**Antes de asumir el empleo**	**Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran**	A.7.1.1	Selección	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar acabo de acuerdo con las leyes reglamentaciones y ética pertinente y deben ser proporcionales a los requisitos de negocio a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos	NO			No procede porque todo el proceso de contratación del personal asignado en las instituciones, es realizado directamente desde las secretarias de educación
			A.7.1.2	Termino y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas deben establecer responsabilidades y las de la organización en cuanto a la seguridad de la información	SI	Tratamiento inadecuado de la información debido a la falta de claridad en las condiciones de trabajo	Establecer procedimientos documentados que garanticen la adecuada verificación de antecedentes y cualificación de las personas que aspiran a realizar trabajos dentro de la institución	

A.7.2	**Durante la ejecución del empleo**	**Asegurarse que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan**	A.7.2.1	Responsabilidades de la dirección	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización	SI	Tratamiento inadecuado de la información debido a la falta de claridad en las condiciones de trabajo	Se debe especificar la responsabilidad de la rectoría en cuanto a la implementación y el mantenimiento del SGSI puesto que hace parte del plan estratégico y a los intereses de sus estudiantes	
			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	SI	Tratamiento inadecuado de la información crítica por desconocimiento de la políticas y procedimientos	Establecer un plan de capacitación de los colaboradores sobre la política de seguridad de la información, así como su evaluación permitirá medir el nivel de conocimiento de los mismo en este tema	

			A.7.2.3	Proceso disciplinario	Se debe contar con un proceso formal el cual debe ser comunicado para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información	SI	No contar con un proceso debidamente documentado, que de las directrices para adelantar procesos disciplinarios en caso de violación en la seguridad de la información	Se debe establecer la penalización disciplinaria que se debe aplicar en caso de infringir las condiciones en cuanto a la seguridad de la información con la que se trabaja	
	Terminación y cambio de empleo	**Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo**	A.7.3.1	Terminación o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo se debe definir, comunicar al empleado o contratista y se debe hacer cumplir	SI	Acceso de información privilegiado por parte de un empleado que ha sido promovido	Se debe establecer términos y condiciones en el momento de la incorporación, permitiendo a la institución protegerse legalmente frente a filtraciones realizadas por trabajadores cesados o promovidos	
A.8	**Gestión de activos**								
COD	**TITULO CONTROL**	**DESCRIPCIÓN OBJETIVO DE CONTROL**	**COD**	**CONTROLES**	**DESCRIPCION DEL CONTROL**	**Aplica Si/No**	**Riesgo**	**ACTIVIDAD**	**OBSERVACIONES**

A.8.1	**Responsabilidad de los activos**	**Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas**	A.8.1.1	Inventarios 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	SI	Perdida de activos por falta de un inventario actualizado	La institución debe manejar un inventario de activos en el que se identifique el tipo de activo y su ubicación.	
			A.8.1.2	Propiedad de los activos	Los activos mantenidos en el inventario deben tener un propietario	SI	Imposibilidad en la asignación de responsabilidades en caso de pérdida o daño de activos	Los activos de información deben ser asignados a un custodio encargado del inventario, clasificación y protección de los activos, así como de la destrucción en caso de que sea necesario, además de la revisión de las restricciones en cuanto a accesos	
			A.8.1.3	Uso aceptable de los activos	Se deben identificar documentar e implementar reglas para el uso aceptable de la	SI	Uso inadecuado de los activos por parte de los propietarios de los mismos	Especificar y documentar a qué se define como uso aceptable en cuanto a manejo	

					información y de activos asociados con información e instalaciones de procesamiento de información			de información personal y sensible mediante una política o procedimiento que debe ser de conocimiento obligatorio para el personal del área	
			A.8.1.4	Devolución de activos	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo	SI	Pérdida de los activos por falta de trazabilidad en préstamo por falta de devolución	Se debe establecer un procedimiento de asignación y devolución de los activos de información, asignado o entregado al personal de la organización	
A.8.2	**Clasificación de la información**	**Asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la organización**	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	SI	Sanciones legales por tratamiento indebido de la información	Realizar una clasificación de los activos identificados según su criticidad para la institución o el nivel de confidencialidad que se le debe otorgar.	

			A.8.2.2	Etiquetado de la información	Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información de acuerdo con el esquema de la clasificación de información adoptado por la organización	SI	Imposibilidad de recuperación de la información necesario o requerida para adelantar procesos críticos de prestación del servicio	Realizar el etiquetado que identifique la información según la clasificación previamente definida, en el caso de los sistemas información los usuarios deberán ver un mensaje visible que indique la clasificación de la información al que accede.	
			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	SI	Manejo inadecuado de activos por carencia de una adecuada clasificación de la información	Establecer procedimientos de manejo de activos de información permitirá que se sigan protocolos que garanticen la seguridad de los mismo.	
A.8.3	**Manejo de medios**	**Evitar la divulgación, la modificación, el retiro o la**	A.8.3.1	Gestión de medios removibles	Se deben implementar procedimientos para gestión de	SI	Copia no autorizada de información	Establecer procedimientos para gestión de	

		destrucción no autorizados de información almacenada en los medios			medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización		crítica de la organización	medios removibles	
			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	SI	Robo de medios	Establecer un protocolo de eliminación de medios que contengan información confidencial, de manera que no pueda ser reutilizado o extraído por personas no autorizadas	
			A.8.3.3	Transferencia de los medios físicos	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el trasporte	SI	Pérdida de la integridad y disponibilidad de información almacenada en medios, causa por un tratamiento indebido o no autorizado por parte de las personas que las custodian o de terceros	Se debe establecer protocolos que aseguren la información en sus transferencias físicas de manera que se garantice su integridad, y que no sea manipulada por personal no autorizado en el momento de salir	

								e ingresar a otro sitio	
A.9	**Control de acceso**								
COD	**TITULO CONTROL**	**DESCRIPCIÓN OBJETIVO DE CONTROL**	**COD**	**CONTROLES**	**DESCRIPCION DEL CONTROL**	**Aplica Si/No**	**Riesgo**	**ACTIVIDAD**	**OBSERVACIONES**
A.9.1	**Requisitos del negocio para control de acceso**	**Limitar el acceso a información y a instalaciones de procesamientos de información**	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	SI	Acceso de personal no autorizado a CPD	Se debe establecer unas políticas donde se documente el acceso a la institución, llevando un control de ingreso y acceso a las áreas críticas	
			A.9.1.2	Acceso a redes y a servicios en red	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente	SI	Acceso de personal no autorizado a información crítica por medio de las conexiones de red	Establecer una política de acceso a nivel de red que establezca los lineamientos en cuanto a segmentación de redes, acceso de externos a la red interna, monitoreo, etc	

A.9.2	**Gestión de acceso a usuarios**	**Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios**	A.9.2.1	Registro y cancelación del registro de usuarios	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios para posibilitar la asignación de los derechos de acceso	SI	Acceso a los activos de información con privilegios disonantes con el perfil del usuario	Para mitigar el riesgo de acceso no autorizado, se debe mantener un procedimiento de alta y sobretodo bajas de usuario de los sistemas de la institución	
			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	SI	Acceso a los activos de información con privilegios disonantes con el perfil del usuario	implementar un proceso de acceso con privilegios a los empleados autorizados, y que permita también retirar ese privilegio en caso de que ya sea necesario	
			A.9.2.3	Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	SI	Acceso a los activos de información con privilegios disonantes con el perfil del usuario	Establecer un proceso de suministro de acceso según las funciones o áreas a las cuales cada empleado pertenece	

			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	SI	Acceso de los activos de información por parte de personal no autorizado	Se debe establecer las directivas de uso de los métodos de autenticación, así como los requisitos para asegurar la confidencialidad de estos datos siento indispensable que estas directivas, se hagan publica a todos los empleados de la institución	
			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	SI	Acceso de los activos de información por parte de personal no autorizado	Los responsables de los activos de información son quienes deben vigilar que empleados puede acceder a los activos de información, además de revisar periódicamente los usuarios que tienen permiso para identificar los que ya no están	

								autorizados a acceder	
			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	SI	Acceso a los activos de información con privilegios disonantes con el perfil del usuario	Los privilegios con los que cuentan los empleados deberán ser eliminados en el caso en que el trabajador, haya cesado su relación con la Institución, o ajustados a lo largo del tiempo en caso en el que el empleado requiera mayores privilegios o ya no los necesite	
A.9.3	**Responsabilidades de los usuarios**	**Hacer que los usuarios rindan cuenta por la salvaguarda de su información de autenticación**	A9.3.1	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	SI	Acceso a los activos de información con privilegios disonantes con el perfil del usuario	Se debe establecer el uso de los métodos de autenticación, así como los requisitos para asegurar la confidencialidad de estos datos.	

A.9.4	**Control de acceso a sistemas de aplicación**	**Evitar el acceso no autorizado a sistemas y aplicaciones**	A9.4.1	Restricción de acceso de información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso	SI	Acceso a los activos de información con privilegios disonantes con el perfil del usuario	Establecer un doble control de autenticación en aquellos sistemas en los que se encuentra información sensible	
			A9.4.2	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	SI	Acceso a sistemas de información por deficiencias en los sistemas de autenticación	Establecer un control enfocado a proteger la información de inicio de sesión del usuario en los sistemas de forma que no pueda ser sustraída por un agente externo	
			A9.4.3	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas	SI	Acceso no autorizado a los sistemas de información	Establecer requisitos mínimos en cuanto a complejidad de contraseñas, los procedimientos de cambios de contraseñas y el almacenamiento de las mismas entre otros	

			A9.4.4	Uso de programas utilitarios privilegiados	Se deben restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones	SI	Parálisis de los servicios de los sistemas de información por el uso de programas utilitarios	Identificar los lineamientos de uso de utilidades ya sean internas o externas, traídas por los empleados a la Institución	
			A9.4.5	Control de acceso a códigos fuente de programas	Se debe restringir el acceso a los códigos fuente de los programas	SI	Instalación de código no autorizado que afecte negativamente la operación de los sistemas de información	Generar cuentas de usuarios restringidos en el equipo informáticos, que no permita que los empleados instalen programas inadecuados	
A.10	**Criptografía**								
COD	**TITULO CONTROL**	**DESCRIPCIÓN OBJETIVO DE CONTROL**	**COD**	**CONTROLES**	**DESCRIPCION DEL CONTROL**	**Aplica Si/No**	**Riesgo**	**ACTIVIDAD**	**OBSERVACIONES**
A.10.1	**Controles criptográficos**	**Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y o**	A10.1.1	Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para protección de la información	SI	Acceso a información privilegiada	Implementar controles y políticas sobre el manejo criptográficos para garantizar la protección de la información	

		la integridad de la información	A10.1.2	Gestión de llaves	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida	SI	Acceso a información privilegiada	Implementar controles y políticas sobre la protección de las llaves criptográficos para garantizar la vida útil de la misma	
A.11	**Seguridad Física y del entorno**								
COD	**TITULO CONTROL**	**DESCRIPCIÓN OBJETIVO DE CONTROL**	**COD**	**CONTROLES**	**DESCRIPCION DEL CONTROL**	**Aplica Si/No**	**Riesgo**	**ACTIVIDAD**	**OBSERVACIONES**
A.11.1	**Áreas seguras**	**Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y las instalaciones de procesamientos de información de la organización**	A11.1.1	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	SI	Intrusión de personas ajenas no autorizadas a las instalaciones físicas	Establecer un límite de acceso físico a los empleados y personal externo a las áreas donde se encuentran la información crítica	
			A11.1.2	Controles de acceso físico	Las áreas seguras que se deben proteger mediante controles de acceso apropiados para asegurar que solo se permita el acceso a personal autorizado	SI	Intrusión de personas ajenas no autorizadas a las instalaciones físicas	Utilizar controles de registro de acceso para el personal que requiera ingresar a los ambientes donde se almacena la información crítica, debe está	

								debidamente identificado en todo momento	
			A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	SI	Intrusión de personas ajenas no autorizadas a las instalaciones físicas	Se debe evitar el acceso de personal no autorizado o al público que hace uso de los servicios de la Institución a los ambientes en los que se almacena información sensible	
			A.11.1.4	Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	SI	Pérdida de activos críticos causado por desastres naturales ataques maliciosos o accidentes	Implementar medidas para proteger la información crítica frente a incidentes que puedan afectar tanto naturales como provocados como los incendios	
			A.11.1.5	Trabajo en áreas seguras	Se deben diseñar y aplicar procedimientos para trabajos en áreas seguras	SI	Sanciones legales o daño en activos	Establecer puntos alejados de las áreas críticas, donde se permita	

								trabajar de forma segura	
			A.11.1.6	Áreas de despachos y carga	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	SI	Intrusión de personas ajenas no autorizadas a las instalaciones físicas	Establecer puntos alejados de las áreas críticas, donde se permita cargar y descargar elementos para la institución,	
A.11.2	**Equipos**	**Prevenir la perdida, daño, robo o compromiso de activos y la interrupción de las operaciones de la organización**	A11.2.1	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	SI	Intrusión de personas ajenas no autorizadas a las instalaciones físicas	Los equipos deben instalarse de manera que se evite el acceso no autorizado a los mismo por parte de personas ajenas al servicio	

			A11.2.2	Servicio de suministros	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	SI	Daños en los equipos por fallas de fluido eléctrico	Los equipos críticos relacionados al manejo de información sensible deben contar con medidas que aseguran su funcionamiento en el caso de caída de algún servicio como el fluido eléctrico	
			A11.2.3	Seguridad de 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	SI	*Daños en los cableados por problemas eléctricos *Interceptación del sistema de registro de estudiantes y tesorería	Adecuar el cableado estructurado, de tal forma que no sea posible intervenir o dañar, interrumpiendo el servicio, o extraer información	
			A11.2.4	Mantenimientos de equipos	Los equipos se deben mantener correctamente para asegurar disponibilidad e integridad continuas	SI	Fallos en la prestación de servicio de tesorería y secretaria académica por problemas en los funcionamientos de los equipos	Los equipos que cuentan con acceso a información crítica deberán seguir un procedimiento de mantenimiento adecuado, de	

								manera que la información que contiene sea comprometida		
			A11.2.5	Retiro de activos	Los equipos de información o software no se deben retirar de su sitio sin autorización previa	SI	Pérdida de los equipos	La institución debe establecer políticas que limiten el retiro de la información sensible de las instalaciones a excepción de ser para cumplir con alguno de los servicios que brinda		
			A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones	SI	Pérdida de los equipos o daños cuando se encuentran fuera de la instaciones	La institución debe asegurar que el uso de la información crítica de la institución que maneja haya sido autorizado por las personas correspondientes		
			A11.2.7	Disposición segura o reutilización de equipos	Se deben verificar todos los elementos de equipos que contengan medios de	SI	Pérdida de información por falta de copias de seguridad	Los equipos que se den de baja o se cambien de área deben hacer pasado por un proceso		

					almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobre escrito en forma segura antes de su disposición o reusó			de limpieza que garantice la eliminación completa de toda la información sensible que pueda contener	
			A11.2.8	Equipos de usuario desatendido	Los usuarios deben asegurar que a los equipos desatendidos se les da protección apropiada	SI	Daños en los equipos	Los empleados deberán mantener la seguridad de sus equipos incluso cuando se levantan del puesto de trabajo para dirigirse a otro sector, o cuando no se está trabajando	
			A11.2.9	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 instaciones de procesamiento de información	SI	Dificultad en la recuperación de información crítica	Los empleados deberán mantener los escritorios libres de cualquier información crítica que pueda ser usada o extraída por persona externo.	

A.12	Seguridad de las operaciones								
COD	**TITULO CONTROL**	**DESCRIPCIÓN OBJETIVO DE CONTROL**	**COD**	**CONTROLES**	**DESCRIPCION DEL CONTROL**	**Aplica Si/No**	**Riesgo**	**ACTIVIDAD**	**OBSERVACIONES**
A.12.1	**Procedimientos operacionales y responsabilidades**	**Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información**	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	SI	Error en los procedimientos de registro académico por falta de información documentada que especifique las actividades relacionadas con dicho registro	Se requiere la documentación de los procesos que se tienen en la institución con el fin de determinar el área más crítica, y realizar una evaluación continua sobre el nivel de riesgo existente, para establecer controles necesarios	
			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.	SI	Pérdida de integridad de la información en el proceso de registro académico	Se deben controlar los cambios en la institución y en los sistemas de procesamiento de información, que afecte la seguridad de la información.	

			A.12.1.3	Gestión de capacidad	Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	SI	Deficiencias en la atención de la comunidad académica por recursos insuficientes	Se debe hacer seguimiento al uso de recursos y establecer si se necesita más recursos para asegurar el desempeño requerido del sistema.	
			A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación	SI	Errores de disponibilidad de la información académica y tesorería por uso de software sin haber realizado pruebas	Se deben separar las áreas, para reducir los riesgos de acceso o cambios no autorizados el área donde se encuentre información crítica	
A.12.2	**Protección contra códigos maliciosos**	**Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas con códigos maliciosos**	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	SI	Interceptación de información por código maliciosos instalado con o sin voluntad por el usuario del sistema	debido al gran avance de amenazas informáticas, la institución deberá asegurar que los equipos de cómputo se encuentren debidamente protegidos ante software	

					códigos maliciosos.			malicioso que ponga en peligro la información sensible de la institución	
A.12.3	**Copias de respaldo**	**Proteger con la pérdida de datos**	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	SI	Perdidas de la continuidad del negocio por daños en los equipos o sistemas de información	Establecer una política de respaldo que garantice la continuidad de la atención y mitigue la pérdida de datos en caso de incidente	
A.12.4	**Registro y seguimiento**	**Registrar eventos y generar evidencia**	A.12.4.1	Registro de eventos	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información	SI	Problemas en sistemas de información sin resolver por falta de información de trazabilidad	Los usuarios que accedan a información crítica deben contar con un login y contraseña con el fin de que se genere un registro de los movimientos realizados por cada usuario	
			A.12.4.2	Protección de la información de registro	Las instalaciones y la información de registro se deben	SI	Acceso no autorizado a la	Los usuarios que accedan a información	

					proteger contra alteración y acceso no autorizado		información de registro	crítica deben contar con un login y contraseña con el fin de que se genere un registro de los movimientos realizados por cada usuario	
			A.12.4.3	Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad	SI	Problemas en sistemas de información sin resolver por falta de información de trazabilidad	Los usuarios que accedan a información crítica deben contar con un login y contraseña con el fin de que se genere un registro de los movimientos realizados por cada usuario	
			A.12.4.4	Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de	SI	Problemas de integridad de información sin resolver por falta de sincronización de los sistemas de información	Realizar una revisión a los equipos para garantizar que estén ajustados a la hora establecida en el país	

					referencia de tiempo				
A.12.5	**Control de software operacional**	**Asegurarse de la integridad delos sistemas operacionales**	A.12.5.1	Instalación de software en sistemas operativos	Se deben implementar procedimiento para controlar la instalación de software en sistemas operativos	SI	Sanciones legales por software pirata	Realizar auditorías periódicas a los equipos informáticos con el fin de identificar software pirata instalados, o que no son permitidos en la institución	
A.12.6	**Gestión de la vulnerabilidad técnica**	**Prevenir el aprovechamiento de las vulnerabilidades técnicas**	A.12.6.1	Gestión de las vulnerabilidades técnicas	Se deben obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado	SI	Acceso no autorizado a información crítica	Se debe establecer una política de revisión periódica para analizar las vulnerabilidades en los equipos donde se almacena información crítica.	

			A.12.6.2	Restricciones sobre la instalación de software	Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios	SI	Sanciones legales por software pirata	Establecer una política que evite que el personal pueda instalar aplicaciones no licenciadas o no permitidas, también se puede restringir las cuentas para que no permita instalar programas	
A.12.7	**Consideraciones sobre auditorías de sistemas de información**	**Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos**	A.12.7.1	Controles de auditorías de sistemas de información	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos de negocio.	SI	Sanciones legales por software pirata	Se debe realizar una auditoría periódica de modo que se verifique el buen funcionamiento y uso de los sistemas de información además de asegurar que solo los usuarios debidamente autorizados cuenten con acceso a la información sensible	
A.13	**Seguridad de las comunicaciones**								

COD	TITULO CONTROL	DESCRIPCIÓN OBJETIVO DE CONTROL	COD	CONTROLES	DESCRIPCION DEL CONTROL	Aplica Si/No	Riesgo	ACTIVIDAD	OBSERVACIONES
A.13.1	**Gestión de la seguridad de las redes**	**Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte**	A.13.1.1	Controles de redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones	SI	Acceso no autorizado a información crítica a través de las redes	La red interna de la institución debe contar con los controles necesarios para asegurar que la información viaje a través de la misma, de modo que no puede ser capturada por un agente externo al flujo de información	
			A.13.1.2	Seguridad de los servicios de red	Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.	SI	Acceso no autorizado a información crítica a través de las redes	Se debe contar con un inventario de servicios de red que establezca los niveles de servicio que deben cumplir además de las características de seguridad con lo que se cuenta	

			A.13.1.3	Separaciones en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	SI	Acceso no autorizado a información crítica a través de las redes	Se deben contar con una correcta separación tanto de redes, como de usuarios en el dominio de la institución que permita verificar los accesos brindados y puedan ser verificados	
A.13.2	**Transferencia de información**	**Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa**	A.13.2.1	Políticas y procedimientos de transferencia de información	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones	SI	Acceso no autorizado a información crítica a través de las redes	Se deben contar con una correcta separación tanto de redes, como de usuarios en el dominio de la institución que permita verificar los accesos brindados y puedan ser verificados	
			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	SI	Acceso no autorizado a información crítica a través de las redes	Durante la transferencia de información se debe especificar a la entidad que la recibe la categoría de la información si es sensible, confidencial o	

								crítica, e indicar mediante un acuerdo de condiciones la confidencialidad de la misma	
			A.13.2.3	Mensajería electrónica	Se debe proteger adecuadamente la información incluida en la mensajería electrónica	SI	Acceso no autorizado a información crítica a través de las redes	Se debe establecer la información que no debe ser divulgada a través de correos electrónicos	
			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	SI	Acceso no autorizado a información crítica a través de las redes	La institución debe establecer acuerdos de confidencialidad que detallen las limitaciones de divulgación de la información por sus empleados	
A.14	**Adquisición, desarrollo y mantenimiento de sistemas**								
COD	**TITULO CONTROL**	**DESCRIPCIÓN OBJETIVO DE CONTROL**	**COD**	**CONTROLES**	**DESCRIPCION DEL CONTROL**	**Aplica Si/No**	**Riesgo**	**Control**	**OBSERVACIONES**

A.14.1	**Requisitos de seguridad de los sistemas de información**	**Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas**	A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes	SI	Acceso no autorizado en los sistemas de información de secretaria académica mediante la explotación de vulnerabilidades	La red interna de la institución debe contar con los controles necesarios para asegurar que la información viaje a través de la misma, de modo que no puede ser capturada por un agente externo al flujo de información	
			A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	SI	Acceso no autorizado a información crítica a través de las redes	La red interna de la institución debe contar con los controles necesarios para asegurar que la información viaje a través de la misma, de modo que no puede ser capturada por un agente externo al flujo de información	
			A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión	SI	Acceso no autorizado a información crítica a través de las redes	La red interna de la institución debe contar con los controles necesarios para asegurar que la información viaje a través de la	

					incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada y la duplicación o reproducción de mensajes no autorizada			misma, de modo que no puede ser capturada por un agente externo al flujo de información	
A.14.2	**Seguridad en los procesos de desarrollo y de soporte**	**Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información**	A.14.2.1	Política de desarrollo seguro	Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización	NO			No se considera dado a que en las instituciones educativas no se realiza desarrollo de software
			A.14.2.2	Procedimientos de control de cambios en sistemas	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios	NO			No se considera dado a que en las instituciones educativas no se realiza desarrollo de software
			A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones	SI	Fallos en la prestación del servicio por falta de pruebas	Se debe solicitar pruebas que garantice que, al realizar cambios de software para operaciones en	

				plataforma de operación	críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización			la institución, no se generen pérdidas o daños a la información, además de realizar una copia de seguridad previa	
			A.14.2.4	Restricciones en los cambios a los paquetes de software	Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente	NO			No se considera dado a que en las instituciones educativas no se realiza desarrollo de software
			A.14.2.5	Principios de construcción de los sistemas seguros	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información	NO			No se considera dado a que en las instituciones educativas no se realiza desarrollo de software
			A.14.2.6	Ambiente de desarrollo seguro	Las organizaciones deben establecer y proteger	NO			No se considera dado a que en las instituciones

					adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas				educativas no se realiza desarrollo de software
			A.14.2.7	Desarrollo contratado externamente	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	NO			No se considera dado a que en las instituciones educativas no se realiza desarrollo de software
			A.14.2.8	Pruebas de seguridad de sistemas	Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad	NO			No se considera dado a que en las instituciones educativas no se realiza desarrollo de software
			A.14.2.9	Prueba de aceptación de sistemas	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para	SI	Fallos en la prestación del servicio por falta de pruebas	Se debe solicitar pruebas que garantice que, al realizar cambios de software para operaciones en la institución, no se generen pérdidas o daños	

					aceptación y criterios de aceptación relacionados.			a la información, además de realizar una copia de seguridad previa	
A.14.3	**Datos de prueba**	**Asegurar la protección de los datos usados para pruebas**	A.14.3.1	Protección de datos de prueba	Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente	SI	Daños en la información original comprometiendo la disponibilidad, integridad y confidencialidad de la información	Se debe solicitar pruebas que garantice que, al realizar cambios de software para operaciones en la institución, no se generen pérdidas o daños a la información, además de realizar una copia de seguridad previa	
A.15	**Relaciones con los proveedores**								
COD	**TITULO CONTROL**	**DESCRIPCIÓN OBJETIVO DE CONTROL**	**COD**	**CONTROLES**	**DESCRIPCION DEL CONTROL**	**Aplica Si/No**	**Riesgo**	**ACTIVIDAD**	**OBSERVACIONES**
A.15.1	**Seguridad de la Información en las relaciones con los proveedores**	**Asegurar la protección de los activos de la organización que sean accesibles a los proveedores**	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	SI	Acceso no autorizado a información crítica	Documentar todos los procesos realizados por los proveedores externos	

					deben acordar con estos y se deben documentar				
			A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con 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	SI	Acceso no autorizado a información crítica	Documentar todos los procesos realizados por los proveedores externos	
			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	SI	Fuga de información de los dicentes por parte de los proveedores que intervienen en los sistemas de información	Realizar auditoria a los servicios prestados por los proveedores de la institución	

A.15.2	**Gestión de la prestación de servicios de proveedores**	**Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores**	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	SI	Fuga de información de los dicentes por parte de los proveedores que intervienen en los sistemas de información	Se debe establecer una política de auditoria permanente a los proveedores de la institución	
			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	SI	Fuga de información de los dicentes por parte de los proveedores que intervienen en los sistemas de información	Realizar auditoria a los servicios prestados por los proveedores de la institución	

A.16	Gestión de incidentes de seguridad de la información								
COD	**TITULO CONTROL**	**DESCRIPCIÓN OBJETIVO DE CONTROL**	**COD**	**CONTROLES**	**DESCRIPCION DEL CONTROL**	**Aplica Si/No**	**Riesgo**	**Control**	**OBSERVACIONES**
A.16.1	**Gestión de incidentes y mejoras en la seguridad de la información**	**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**	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	SI	Pérdida de imagen por no atención oportuna por daños en los activos	Se debe detallar las responsabilidades y procedimientos correspondientes a dicho equipo de manera que se encuentren debidamente identificadas las funciones del mismo	
			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	SI	Pérdida de imagen por no atención oportuna por daños en los activos	Realizar revisiones para identificar eventos o vulnerabilidades y deben ser reportados para su análisis	
			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	SI	Pérdida de imagen por no atención oportuna por daños en los activos	Realizar revisiones para identificar eventos o vulnerabilidades y deben ser reportados para su análisis	

					debilidad de seguridad de la información observada o sospechada en los sistemas o servicios				
			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	SI	Pérdida de imagen por no atención oportuna por daños en los activos	Analizar los eventos encontrados por el equipo, determinando las acciones para evitar incidentes	
			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	SI	Pérdida de imagen por no atención oportuna por daños en los activos	Establecer procedimientos para evitar eventos y vulnerabilidades que se han presentado o se puedan presentar	
			A.16.1.6	Aprendizajes obtenidos de los incidentes de seguridad de la información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se de usar para reducir la posibilidad o el impacto de incidentes futuros	SI	Pérdida de imagen por no atención oportuna por daños en los activos	Se debe documentar y dejar historial de todos los eventos que se identifiquen en una bitácora, con el fin de ayudar a disminuir ocurrencias futuras	

			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.	SI	Pérdida de imagen por no atención oportuna por daños en los activos	Se debe recolectar todas las evidencias de los incidentes presentados.	
A.17	**Aspectos de seguridad de la información de la gestión de continuidad de negocio**								
COD	**TITULO CONTROL**	**DESCRIPCIÓN OBJETIVO DE CONTROL**	**COD**	**CONTROLES**	**DESCRIPCION DEL CONTROL**	**Aplica Si/No**	**Riesgo**	**ACTIVIDAD**	**OBSERVACIONES**
A.17.1	**Continuidad de seguridad de la información**	**La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización**	A.17.1.1	Planificación de la continuidad de la seguridad de la información	La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre	SI	No se presta el servicio de registro académico permanentemente a los usuarios a consecuencia de un desastre natural	La institución deberá identificar los activos de información que son críticos para asegurar la continuidad de las operaciones de la institución, según el impacto de disponibilidad del servicio que tendría una pérdida de dicha información	

			A.17.1.2	Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa	SI	No se presta el servicio de registro académico permanentemente a los usuarios a consecuencia de un desastre natural	Establecer que los planes de contingencia la protección de los activos de información previamente identificados, de manera que se asegure la disponibilidad de los mismo haciendo más eficiente la recuperación de los servicios de la institución	
			A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas	SI	No se presta el servicio de registro académico permanentemente a los usuarios a consecuencia de un desastre natural	Establecer la realización de pruebas periódicas para verificar que los planes de contingencia establecidos, así como el nivel de protección de la información esté disponible frente a los distintos escenarios que haya presentado.	

A.17.2	**Redundancias**	**Asegurar la disponibilidad de instalaciones de procesamiento de información**	A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad	SI	Ausencia de información crítica redundante que garantice la disponibilidad y la continuidad de los procesos críticos (registro académico y tesorería)	La institución debe establecer servidores que almacene la información sensible o crítica para las operaciones, además deberán contar con instalaciones alternas en las cuales se almacene la información de manera redundante, con el fin de recuperar la información en caso de una emergencia	
A.18	**Cumplimiento**								
COD	**TITULO CONTROL**	**DESCRIPCIÓN OBJETIVO DE CONTROL**	**COD**	**CONTROLES**	**DESCRIPCION DEL CONTROL**	**Aplica Si/No**	**Riesgo**	**Control**	**OBSERVACIONES**
A.18.1	**Cumplimiento de requisitos legales y contractuales**	**Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales**	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	SI	Sanciones legales por uso inadecuado de la información de conformidad por lo dispuesto por el MEN	La institución debe contar con documentación alusivos a la normativa relacionada a seguridad de la información que	

		relacionadas con seguridad de la información y de cualquier requisito de seguridad			cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización			afecta a la institución	
			A.18.1.2	Derechos de propiedad intelectual	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados	SI	Sanciones legales por uso inadecuado de la información de conformidad por lo dispuesto por la legislación de derechos de autor	implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados	
			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	SI	Sanciones legales por uso inadecuado de la información de conformidad por lo dispuesto por el MEN y la ley de habeas data	La institución debe contar con procedimiento que determinen las condiciones de almacenamiento de información física, el periodo de tiempo por el	

					requisitos legislativos de reglamentación, contractuales y de negocio			cual dicha información debe ser almacenada y los procedimientos estándar de desecho de información	
			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.	SI	Sanciones legales por uso inadecuado de la información de conformidad por lo dispuesto por el MEN y la ley de habeas data	La institución debe garantizar que la información personal de la población deberá ser protegida de acuerdo a lo indicado por la Ley de protección de datos personales	
			A.18.1.5	Reglamentación de controles criptográficos	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes	SI	Sanciones legales por uso inadecuado de la información de conformidad por lo dispuesto por el MEN y la ley de habeas data	Se debe establecer controles para el uso de criptografía en cumplimiento de todos los acuerdos y reglamentación.	

A.18.2	**Revisiones de seguridad de la información**	**Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales**	A.18.2.1	Revisiones independientes de la seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos	SI	Ausencia de controles alineados a la realidad operativa de la seguridad de la información por falta de revisiones periódicas	El sistema de Gestión de Seguridad de la información deberá ser revisado periódicamente teniendo en cuenta los cambios organizacionales o legislativos que se produzcan	
			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	SI	Ausencia de controles alineados a la realidad operativa de la seguridad de la información por falta de revisiones periódicas	Las políticas de Seguridad de la Información deberán ser evaluadas periódicamente en cuanto a su cumplimiento en la institución, así como ajustados de acuerdo a los cambios que se puedan hacer producido en el	

					requisito de seguridad			marco legal u organizacional	
			A.18.2.3	Revisión del cumplimiento técnico	Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información	SI	Ausencia de controles seguridad de la información alineados a la realidad operativa de la seguridad de la información por falta de revisiones periódicas	Los sistemas de información utilizados deben ser evaluados periódicamente en cuanto al cumplimiento de los aspectos técnicos relacionados con las políticas de seguridad de modo que se puedan detectar fallas o vulnerabilidades nuevas.	

CONCLUSIONES

De acuerdo a los resultados obtenidos durante todo el proceso y elaboración del proyecto de grado, se pudo determinar el grado de madurez de los controles de la norma ISO/IEC 27001:2013 Seguridad de la Información, quedando ubicado en un nivel crítico, y en la fase inicial de madurez de los controles.

Es importante señalar que se evidencio poco conocimiento por parte de los colaboradores en torno a la cultura de vigilar y asegurar la información, siendo vulnerables a las perdidas y fallos de los equipos informáticos, por otra parte hace falta más capacitación en cuanto al manejo de las herramientas tecnológicas, debido a que por falta de conocimientos fue posible extraer información desde la web, documentos que son netamente institucionales, además de encontrar equipos que no cuentan con usuario y contraseña para acceder al equipo, siendo de fácil acceso para personal externo, asimismo los equipos informáticos cuentan con poca protección, debido a que son vulnerables a los ataques informáticos.

Es de suma importancia que las instituciones Educativas adopten políticas de seguridad, y que se implemente un Sistema de Gestión de seguridad de la información que garantice la confidencialidad, integridad y seguridad de los datos.

Realizar auditorías de manera periódica permite identificar el nivel de seguridad en que se hallan los activos de información en la institución, permitiendo desarrollar alternativas o estrategias de implementación, metodologías o estructuras, que permitan mitigar las amenazas, riesgos y vulnerabilidades a las que se someten día a día los activos informáticos, generando daños irreversibles en las instituciones

RECOMENDACIONES

Dada la necesidad de implementar un Sistemas de Gestión de Seguridad de la Información SGSI en instituciones educativas públicas del nivel preescolar en este documento se diagnosticó el grado de madurez de los controles de seguridad con base en la norma ISO 27001:2013 con el fin de que sea un punto de partida para definir un modelo para el diseño de SGSI para el nivel preescolar de las instituciones educativas de la comuna Universidad de la ciudad de Pereira.

Por esta razón se realiza las siguientes recomendaciones:

1. Implementar un SGSI

2. Realizar la documentación de procesos para poder gestionar los mismo de manera óptima y hacer frente a cualquier cambio

3. Generar constantemente revisiones a la política del SGSI

4. Concientizar al personal de la importancia de cumplir con las políticas establecidas del SGSI, además de realizar auditorías periódicas a los procesos establecidos y al personal responsable de dichos procesos.

5. Establecer mecanismos con el fin de identificar los activos de información nuevos, además de generar la cultura organizacional con el fin de garantizar la toma de acciones correctivas frente a nuevas vulnerabilidades, riesgos y amenazas detectados, al igual que la toma de acciones preventivas.

6. Realizar de forma periódica análisis de riesgos, logrando de esta manera identificar nuevas vulnerabilidad y amenazas que afecten los activos de información, tomando medidas preventivas evitando así generar nuevamente la brecha de incumplimiento de la norma.

7. Capacitar periódicamente al personal con el fin de formarlos en SGSI, logrando que todos se involucren o relacionen con los temas de Seguridad de los activos de información teniendo los alcances claros de implementación

8. Programar capacitaciones constantemente al personal en manejo básico de sistemas y concientizar de la importancia de bloquear el equipo al momento de ausentar de su puesto de trabajo

REFERENCIAS BIBLIOGRAFICAS

Calvo García, Á. L. (2014). Gestión de Redes Telemáticas. IFCT0410. ANTEQUERA, Málaga: IC Editorial.

Caviedes Sanabria, F., & Prado Urrego, B. A. (2012). Modelo unificado para identificación y valoración de los riesgos de los activos de información en una organización. Obtenido de Modelo unificado para identificación y valoración de los riesgos de los activos de información en una organización: https://bibliotecadigital.icesi.edu.co/biblioteca_digital/bitstream/10906/68413/1/modelo_unificado_identificacion.pdf

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

Condori Benavides, I. (2015). Control Interno. Perú: Universidad Autónoma.

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

Decreto 1075. (2015). Por medio del cual se expide el Decreto Unico Reglamentario del Sector Educación. 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.

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.

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

ISACA. (2013). COBIT 5 FOR RISK. Rolling Meadows.

ISO 27000.ES. (2005). El portal de ISO 27001 en Español. Obtenido de El portal de ISO 27001 en Español: http://www.iso27000.es/sgsi.html

ISO/IEC 27000. (2014). Términos y Definiciones. Bogotá.

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

Koenig, S. (7 de Marzo de 2016). Movimiento de los Pueblos para la Educación en Derechos Humanos. Obtenido de Movimiento de los Pueblos para la Educación en Derechos Humanos: http://www.pdhre.org/rights/education-sp.html

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 la Presidencia. (2010). Legislación consolidad. España.

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.

Torres Bermúdez, A. A. (2010). Introducción a la Seguridad Informática.

GLOSARIO

Activo
En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistema, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000, Tomado de Modelo de Seguridad y Privacidad de la Información).

Amenazas
Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización (ISO/IEC 27000, Tomado de Modelo de Seguridad y Privacidad de la Información)

Análisis de Riesgo
Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo (ISO/IEC 27000, Tomado de Modelo de Seguridad y Privacidad de la Información)

Auditoría
Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria (ISO/IEC 27000, Tomado de Modelo de Seguridad y Privacidad de la Información)

Ciberseguridad
Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701, Tomado de Modelo de Seguridad y Privacidad de la Información)

Ciberespacio
Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701, Tomado de Modelo de Seguridad y Privacidad de la Información)

Control
Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo. (Tomado de Modelo de Seguridad y Privacidad de la Información)

Declaración de aplicabilidad
Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información - SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, asi como la

justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000, Tomado de Modelo de Seguridad y Privacidad de la Información)

Gestión de incidentes de seguridad de la información
Proceso para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000, Tomado de Modelo de Seguridad y Privacidad de la Información)

Plan de tratamiento de riesgos
Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000, Tomado de Modelo de Seguridad y Privacidad de la Información)

Riesgo
Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000, Tomado de Modelo de Seguridad y Privacidad de la Información)

Seguridad de la información
Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000, Tomado de Modelo de Seguridad y Privacidad de la Información)

Vulnerabilidad
Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000, Tomado de Modelo de Seguridad y Privacidad de la Información)