DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL COLEGIO GERMÁN ARCINIEGAS I.E.D., BAJO LA NORMA TÉCNICA COLOMBIANA NTC ISO/IEC 27001:2013.

ING. CAROLINA FIGUEROA CUBILLOS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C., COLOMBIA
2018

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL COLEGIO GERMÁN ARCINIEGAS I.E.D., BAJO LA NORMA TÉCNICA COLOMBIANA NTC ISO/IEC 27001:2013.

ING. CAROLINA FIGUEROA CUBILLOS

TRABAJO DE GRADO PARA OPTAR AL TÍTULO DE ESPECIALISTA EN SEGURIDAD INFORMÁTICA.

DIRECTOR: PHD(C). GABRIEL MAURICIO RAMÍREZ VILLEGAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C., COLOMBIA
2018

Nota de aceptación:

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bogotá D.C., 24 de octubre de 2018

AGRADECIMIENTOS

Agradezco a Dios dueño de mi vida, a mi esposo Freddy y a mis hijos Freddy Nicolay, Daniela y Ana María, por estar a mi lado siempre y apoyarme en este proceso.

Agradezco a la Dra. Sorangela Miranda Beltrán, rectora del colegio Germán Arciniegas, a mis compañeros administrativos por todo el apoyo recibido para el buen desarrollo del proyecto y a la comunidad educativa germanista por permitirme dar a conocer el proyecto del Sistema de Gestión de Seguridad de la Información para el colegio Germán Arciniegas.

Para finalizar y sin ser menos importante, agradezco al Ingeniero Gabriel Mauricio Ramírez Villegas, por su asesoría y valiosos aportes como director del proyecto "Diseño de un sistema de gestión de seguridad de la información para el colegio Germán Arciniegas I.E.D., bajo la norma técnica colombiana NTC ISO/IEC 27001:2013.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág

LISTA DE FIGURAS

Pág

GLOSARIO

El siguiente Glosario fue tomado como referencia del programa Gobierno en Línea[1].

ACCESIBILIDAD: La posibilidad de acceder universal a la Web, independientemente del tipo de hardware, software, infraestructura de red, idioma, cultura, localización geográfica y capacidades de los usuarios.

ACTIVISMO DIGITAL: Ejercicio de la ciudadanía y del compromiso social mediante la participación en redes sociales de personas naturales o jurídicas creando dinámicas de información, sensibilización, educación y movilización social usando la web.

ACTIVO: Cualquier cosa que tiene valor para la organización NTC-ISO /IEC 27001.

ANÁLISIS DE RIESGO: Uso sistemático de la información para identificar las fuentes y estimar el riesgo NTC-ISO /IEC 27001.

AUTOMATIZAR: Hace referencia a la incorporación de herramientas tecnológicas a un proceso o sistema.

BACK OFFICE: Hace referencia a la parte donde tienen lugar las tareas destinadas a la gestión de la propia empresa y con las cuales el cliente no tiene un contacto directo. En el ámbito tecnológico, se refiere a los sistemas automáticos que respaldan las acciones que acompañan a una transacción.

BACKUP: Copia de seguridad de uno o varios archivos digitales o informáticos que ayuda a prevenir posibles pérdidas en la información.

CONFIDENCIALIDAD: Propiedad de la información que determina que esté disponible a personas autorizadas.

CONJUNTO DE DATOS: Es un conjunto de variables y datos asociados.

CYBERSTALKING: Es el acoso, espionaje o persecución que se da a una persona o grupo usando Internet u otro dispositivo electrónico. Este acoso puede darse con investigación constante de información sobre la persona, acusaciones falsas, espionaje, amenazas, robo de identidad y daño a la información o el equipo que la almacena.

---

[1] GOBIERNO DIGITAL, Glosario. [En línea]. Bogotá: Ministerio de Tecnologías de la Información y las Comunicaciones. 2018. Disponible en: http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7742.html

CIBERDELINCUENTE: persona que comete actos ilícitos que implican el uso de ordenadores o de internet.

CIBERDELITO: Actos criminales, delictivos o ilícitos que implican el uso de ordenadores o de internet.

CRACKERS: Son aquellas personas con muchos conocimientos en los sistemas de información pero utilizan con malas buenas intenciones, rompen la seguridad de los sistemas.

DISPONIBILIDAD: Propiedad de que la información y sus recursos relacionados deben estar disponibles y utilizables cuando se los requiera. Entendida en un documento electrónico, como la capacidad actual y futura de que tanto el documento como sus metadatos asociados puedan ser consultados, localizados, recuperados, presentados, interpretados, legibles y por tanto estar en condiciones de uso.

DOCUMENTO ELECTRÓNICO: es la información generada, enviada, recibida, almacenada y comunicada por medios electrónicos, ópticos o similares[2].

EN TIC CONFÍO: Programa del Ministerio TIC que busca promover usos increíbles, productivos, creativos, seguros, respetuosos y responsables de las TIC; que contribuyan a mejorar la calidad de vida de todas y todos los colombianos.

EVALUACIÓN DEL RIESGO: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo. NTC-ISO /IEC 27001.

FIABILIDAD: Entendida como la capacidad de un documento para asegurar que su contenido es una representación completa, fidedigna y precisa de las operaciones, las actividades, los hechos que testimonia o se puede establecer, declarar o sostener el acto o hecho del que es relativo, determinando la competencia del autor y examinando tanto la completitud en la forma del documento como el nivel de control ejercido durante su proceso de producción.

FLAMING: Es cuando una discusión que se lleva a cabo en línea (en correos electrónicos, redes, blogs o foros) toma un tono insultante, burlón o desagradable hacia una de las personas con el objetivo de enojarla e imponer los puntos de vista de la otra.

---

[2] G.INF.07 Guía para la gestión de documentos y expedientes electrónicos, Guía Técnica, versión 1.0, 14 de noviembre de 2017, Ministerio de las Tecnologías de la Información y las Comunicaciones y del Archivo General de la Nación.

GROOMING: Es cuando un posible abusador o pedófilo trata de iniciar una relación en línea con un menor de edad, buscando involucrarlo en actos sexuales, intercambio de imágenes y en conversaciones con contenido sexual.

HACKER: es aquella persona que cuenta con amplios conocimientos en áreas de informática, especialmente en seguridad o programación.

HACKEAR: Es el ingreso ilegal a computadores, páginas y redes sociales con el objetivo de robar información, suplantar la identidad del dueño, beneficiarse económicamente o protestar.

INTEGRIDAD: Propiedad de salvaguardar la exactitud de la información y sus métodos de procesamiento deben ser exactos.

MALWARE: Es software malicioso, todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.

NEWBIE: Es el novato que se tropieza con una página web sobre Hacking y baja todas las utilidades y programas a su PC, comienza a leer y ejecutar los programas para ver que hacen. Es un principiante inofensivo en busca de más información sobre Hacking.

OPEN DATA: Datos Abiertos corresponde a una filosofía y práctica que persigue que determinados datos de los Gobiernos estén disponibles de forma libre a todo el mundo, sin restricciones de copyright, patentes u otros mecanismos de control, permitiendo el impulso del crecimiento económico, salvaguardar los derechos de ciudadanos y empresas, así como, delimitar las obligaciones de las administraciones.

PHISHING: Es un delito cibernético con el que por medio del envío de correos se engaña a las personas invitándolas a que visiten páginas web falsas de entidades bancarias o comerciales. Allí se solicita que verifique o actualice sus datos con el fin de robarle sus nombres de usuarios, claves personales y demás información confidencial.

PORNOGRAFÍA INFANTIL: Es toda representación visual, gráfica, de texto, dibujos animados o videojuegos, que de manera real o simulada, explícita o sugerida, involucran la participación de menores de edad o personas que aparenten serlo, en el desarrollo de actividades sexuales.

REGISTRO: Información de fecha, hora, destinatario y consecutivo que se asigna a través del Sistema de Gestión Documental, a las respuestas generadas para las PQR y Derechos de Petición.

SERVICIO EN LÍNEA: Servicio que puede ser prestado por medios electrónicos a

través del portal de una entidad.

SEXTING: Es cuando alguien toma una foto poco apropiada de sí mismo (sugestiva o sexualmente explícita), y la envía a alguien vía teléfono celular o Internet.

SEXTORSIÓN: Es la amenaza de enviar o publicar imágenes o videos con contenido sexual de una persona. Esto puede hacerse a través de teléfonos celulares o Internet.

SGD: Sistema de Gestión Documental se refiere a un repositorio de documentos de una entidad, este repositorio cuenta con índices e información que permite el uso, localización y almacenamiento de los documentos.

SPOOFING: Hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación, sin que la víctima lo detecte.

TI: Tecnologías de la Información. Hace referencia a las aplicaciones, información e infraestructura requerida por una entidad para apoyar el funcionamiento de los procesos y estrategia de negocio.

TIC: Tecnologías de la Información y las Comunicaciones, son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes (Art. 6 Ley 1341 de 2009).

TRÁMITE EN LÍNEA: Trámite que puede ser realizado por medios electrónicos a través del portal de una entidad, ya sea de manera parcial, en alguno de sus pasos o etapas, o total, hasta obtener completamente el resultado requerido.

USABILIDAD: Se refiere a la rapidez con que se puede aprender a utilizar algo, la eficiencia al utilizarlo, cuán memorable es, cuál es su grado de propensión al error, y cuánto les gusta a los usuarios.

USUARIO: Persona o máquina delegada por un cliente para utilizar los servicios y/o facilidades de una red de telecomunicaciones.

VISHING: Consiste en hacer llamadas telefónicas a las víctimas, en las que por medio de una voz computarizada, muy similar a las utilizadas por los bancos, se solicita verificar algunos datos personales e información bancaria.

RESÚMEN

Teniendo en cuenta el aumento significativo y la evolución de los delitos informáticos, los ciberdelincuentes se han organizado y fortalecido en sus ataques; las grandes empresas que generan mayor rentabilidad para los delincuentes son sus principales víctimas y "en cuanto a las tipologías criminales, las denunciadas ante la Policía Nacional en el citado periodo de tiempo, se evidencia un aumento significativo en el número de estas por conductas delictivas que vulneraron la integridad personal, patrimonio económico de entidades públicas y privadas, así como la integridad, disponibilidad y confidencialidad de la información que circula a través del ciberespacio" [3]

Se realizará el diseño de un sistema de gestión de la seguridad de la información, para el Colegio Germán Arciniegas I.E.D., bajo la norma técnica colombiana NTC-ISO-IEC 27001:2013, que permita el aseguramiento de la información mediante el reconocimiento de la institución sus necesidades, expectativas, la identificación de las partes interesadas, determinación del alcance del sistema dentro de la organización, la definición de la política de seguridad, de los roles y de las responsabilidades frente al sistema.

Por otra parte, se identificarán y analizarán los riesgos a los que se encuentran expuestos los sistemas informáticos de la institución y la información en general; adicionalmente, se realizarán los planes de acción para tratar estos riesgos y se definirán los objetivos para cumplir con el sistema de seguridad de la información.

Finalmente, el sistema proveerá de medidas preventivas, procesos y controles para la seguridad de la información que garantice la disponibilidad, confiabilidad, e integridad de la información en el colegio Germán Arciniegas. Esto se llevará a cabo mediante la recolección la información en cada una de las áreas de la IED, la realización el inventario de los activos informáticos de la Institución, el análisis de riesgos y la definición de procesos de seguridad de la información en la IED, acorde con las directrices dadas en la NTC-ISO-IEC 27001:2013 y la definición de los procesos de seguridad de la información generada en la IED.

[3] INFORME AMENAZAS DEL CIBERCRIMEN EN COLOMBIA 2016 – 2017. [En línea]. Bogotá: Centro Cibernético Policial. 2017., 15 P. Disponible en https://caivirtual.policia.gov.co/contenido/informe-amenazas-del-cibercrimen-en-colombia-2016-2017.

INTRODUCCIÓN

Dada la evolución, la manera organizada y el fortalecimiento de los delincuentes en sus ataques informáticos; el aumento significativo de conductas delictivas que vulneran la integridad personal, la economía de empresas, así como la integridad, de la información, que son los ataques denunciados ante la Policía Nacional, donde las principales víctimas son grandes empresas de sectores público y privado, que generan mayor rentabilidad en la actividad delictiva.

El Colegio Germán Arciniegas I.E.D., que pertenece al nivel institucional de la Secretaría de Educación Distrital (SED)[4], mediante Resolución SED No. 161 del 24 de enero de 2008, como entidad que forma parte de la administración pública, se compromete con el establecimiento de políticas y objetivos de la seguridad de la información, en concordancia con los principios de seguridad y privacidad de la información y la normativa vigente, mediante el diseño de un sistema de gestión de la seguridad de la información, bajo la norma técnica colombiana NTC-ISO-IEC 27001:2013, con el fin de prevenir riesgos, racionalizar trámites, ofreciendo accesibilidad a su trámites y servicios.

La institución educativa adopta las políticas de seguridad de la información de la Secretaría de Educación del Distrito, mediante la Resolución 1944 de 2016, en la cual se considera:

> Que el Decreto Único Reglamentario del Sector de Tecnologías de la Información y la Comunicaciones, dispone que las entidades que conforman la administración pública serán sujetos obligados al cumplimiento de las políticas y los lineamientos de la Estrategia de Gobierno en Línea y estableció como uno de sus cuatro componentes el de la Seguridad y Privacidad de la Información comprendido por las acciones trasversales a los componentes de TIC para Servicios, TIC para el Gobierno Abierto y TIC para la Gestión, tendientes a proteger la información y sistemas de información, del acceso, divulgación, interrupción o destrucción no autorizada [5].

Para el desarrollo del diseño del SGSI, se llevará a cabo la recolección de la información de los procesos realizados en cada una de las áreas de la I.E.D., con lo que se pretende realizar una caracterización de estos procesos, la realización del inventario de los activos informáticos de la Institución, el análisis de riesgos, la

---

[4] SECRETARÍA DE EDUCACIÓN DEL DISTRITO. Resolución No. 161. (24, enero, 2008). Por la cual se separa del Colegio Basilia la sede de ampliación Brasil López Quintana, tomando el nombre de Colegio Germán Arciniegas.

[5] COLOMBIA. SECRETARÍA DE DUCACIÓN DEL DISTRITO. Resolución 1944. (26, diciembre, 2016). Por medio de la cual se adopta la Política de Seguridad de la Información de la Secretaría de Educación del Distrito. Registro Distrital 5982. Bogotá. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=68201

definición y estandarización de los procesos de seguridad de la información en la IED, acorde con las directrices dadas en la NTC-ISO-IEC 27001:2013[6].

Se tendrán en cuenta la normatividad vigente y los lineamientos, normas y guías establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, que permiten estructurar el diseño del sistema de gestión de la seguridad de la información que se realizará para el Colegio Germán Arciniegas I.E.D. bajo la norma técnica colombiana NTC-ISO-IEC 27001:2013, dentro del ciclo PHVA solo se realizará la planeación no incluye la implementación, evaluación ni mejora.

[6] INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Sistemas de gestión de la seguridad de la Información: técnicas de seguridad y requisitos. NTC-ISO/IEC 27001. Bogotá D.C.: El Instituto, 2013. 26 p.

1. DEFINICIÓN DEL PROBLEMA DE INVESTIGACION

1.1. ANTECEDENTES DEL PROBLEMA

Los delitos informáticos han evolucionado de manera exponencial, a tal punto que los ciberdelincuentes se han organizado de tal manera que han creado organizaciones muy complejas y trasnacionales, de acuerdo con el informe presentado por el CAI virtual de la Policía Nacional[7].

En Colombia se registran diariamente más de 542 mil ataques informáticos y en el último año, se presentaron más de 198 millones de incidentes y nadie está exento de ser víctima de un ciberataque, pueden ser grandes, medianas o pequeñas empresas; empresas gubernamentales o ciudadanos del común. Si bien es cierto que el sector financiero es el más afectado por los ataques informáticos en Colombia, el sector gubernamental ocupa el tercer puesto seguido del sector de telecomunicaciones[8].

Aunque una de las principales conclusiones en el Informe "Impacto de los incidentes de seguridad digital en Colombia 2017", se evidencia que la mayoría de las organizaciones de Colombia entrevistadas se encuentran preparadas para responder a un ataque cibernético, sin embargo se requiere seguir invirtiendo en más seguridad digital para estar a la altura de los desafíos que plantea la ciberdelincuencia en el Siglo XXI, y el estudio advierte sobre los pocos recursos que le dedican las empresas a la seguridad digital.

Por otra parte, este estudio reveló que, en "los ataques recibidos por las entidades, se identificaron cuatro riesgos comunes: Phishing, Malware, DoS y Ataques basados en web. En el estudio se observó que, dentro del sector de Servicios, el 50% de los que respondieron notaron un aumento en los ataques de malware, 47% de phishing, 39% de ataques basados en web y 18% de ataques de denegación de servicio"[9]. Durante los años 2014, 2015, 2016 y al 10 de marzo del 2017, se recibieron 13.774 denuncias por violación a la ley 1273 de 2009, dando un panorama de los delitos que más se denuncian en el país.

De acuerdo con las denuncias realizadas ante el CAI virtual de la Policía Nacional en los últimos años, se evidencia el incremento de las conductas delictivas que atacan la integridad personal, economía de las empresas, así como la integridad,

---

[7] Ibíd., p. 1.

[8] Publicación del Tiempo, del 27 de septiembre de 2017 en http://www.eltiempo.com/tecnosfera/novedades-tecnologia

[9] Organización de los Estados Americanos (OEA), el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MINTIC) y el Banco Interamericano de Desarrollo (BID). Informe Impacto de los incidentes de seguridad digital en Colombia 2017. [En línea]. 2017. Disponible en https://publications.iadb.org/handle/11319/8552?locale-attribute=es&.

de la información que se publica en la web, “siendo el Artículo 269I, hurto por medios informáticos y semejantes, la tipología criminal de mayor frecuencia, equivalente al 68%, seguido de Artículo 269ª, acceso abusivo a un sistema informático con el 13% y “Artículo 269F violación de datos personales con 12% de la muestra”[10].

1.2. DESCRIPCIÓN DEL PROBLEMA

Teniendo en cuenta que en el Acuerdo Distrital 257 de 2006, en su Artículo 5, párrafo 3, se establece que “las actuaciones administrativas serán públicas, soportadas en tecnologías de información y comunicación, de manera que el acceso a la información oportuna y confiable, facilite el ejercicio efectivo de los derechos constitucionales y legales y los controles ciudadano, político, fiscal, disciplinario y de gestión o administrativo sin perjuicio de la reservas legales” [11], el uso de las tecnologías de la información son un canal utilizado por la institución como medio de comunicación donde el Colegio Germán Arciniegas por ser una Institución Educativa Distrital, se acoge a la normas legales vigentes.

La Secretaría de Educación Distrital, ha manifestado su compromiso con el establecimiento de políticas y objetivos de la seguridad de la información, de acuerdo con los principios de seguridad y privacidad de la información y la normatividad vigente, con el fin de prevenir riesgos, racionalizar trámites y ofreciendo mayor acceso a los trámites y servicios en línea de los niveles central, local e institucional.

Actualmente en la ciudad de Bogotá Distrito Capital, se cuenta con 2241 Instituciones Educativas reguladas por la Secretaría de Educación del Distrito, clasificadas entre colegio oficiales y no oficiales; de los colegios oficiales se tienen los colegios distritales, en concesión y de régimen especial y de los colegio no oficiales se tienen los colegios privados, privado con matrícula contratada y privado de régimen especial. A continuación en la tabla 1, se relacionan las cantidades de colegios existentes por localidad, esta información se tomó del directorio único de establecimientos educativos de Bogotá[12].

[10] Cifras SIEDCO - Plataforma Estadística se Criminalidad y Operatividad de la Policía Nacional. A fecha 10/03/2017.

[11] COLOMBIA. CONCEJO DE BOGOTÁ D.C. Acuerdo 257. (30, noviembre, 2006). Por el cual se dictan normas básicas sobre la estructura, organización y funcionamiento de los organismos y de las entidades de Bogotá Distrito Capital, y se expiden otras disposiciones. Registro Distrital 3662. Bogotá D.C. El Consejo. 2006. 31 p. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=22307

[12] SECRETARÍA DE EDUCACIÓN DEL DISTRITO. Directorio único de establecimientos educativos de Bogotá. [En línea]. (2018). Disponible https://dueb.educacionbogota.edu.co/Dueb/colegioListado.sed

Tabla 1. Cantidad de colegios por localidad.

		COLEGIOS OFICIALES			COLEGIOS NO OFICIALES			
No.	LOCALIDAD	DISTRITALES	DISTRITALES EN CONCESIÓN	RÉGIMEN ESPECIAL	PRIVADO	PRIVADO MATRICULA CONTRATADA	PRIVADO RÉGIMEN ESPECIAL	TOTAL
1	Usaquén	11	1	3	124	0	0	139
2	Chapinero	3	0	0	26	0	0	29
3	Santa Fe	8	1	0	18	0	2	29
4	San Cristóbal	33	2	0	78	0	0	113
5	Usme	45	4	0	45	0	0	94
6	Tunjuelito	12	0	1	49	0	1	63
7	Bosa	28	5	0	75	12	0	120
8	Kennedy	42	2	1	205	7	0	257
9	Fontibón	11	0	0	98	0	0	109
10	Engativá	33	2	0	250	6	2	293
11	Suba	26	2	1	339	18	1	387
12	Barrios Unidos	9	0	2	59	0	0	70
13	Teusaquillo	2	0	2	85	0	0	89
14	Los Mártires	8	0	1	30	0	0	39
15	Antonio Nariño	5	0	0	44	0	0	49
16	Puente Aranda	15	0	0	89	0	0	104
17	La Candelaria	2	0	0	16	0	0	18
18	Rafael Uribe	27	1	0	84	3	1	116
19	Ciudad Bolívar	40	2	0	69	10	0	121
20	Sumapaz	2	0	0	0	0	0	2
	TOTAL	362	22	11	1783	56	7	2241

Fuente el autor.

Teniendo en cuenta que la Secretaría de Educación del Distrito en su nivel institucional cuenta con 395 colegios oficiales, la información que cada una de estas instituciones tiene a su cargo es manipulada de manera autónoma y aunque la SED ha realizado esfuerzos en la construcción de sistemas de gestión, actualmente no se cuenta con un diseño para la seguridad de la información en las instituciones educativas.

Actualmente, el colegio Germán Arciniegas no cuenta con el diseño ni la implementación de un sistema de gestión de seguridad de la información, lo cual implica que la institución educativa sea vulnerable ante amenazas y se encuentre

expuesta a riesgos que puedan generar pérdida en la información, alteración de los contenidos, daños en equipos informáticos y mal servicio en las aplicaciones en línea.

Teniendo en cuenta que el colegio Germán Arciniegas es una institución que forma parte del nivel institucional de la Secretaría de Educación, el diseño del sistema de gestión de seguridad de la información del colegio, debe estar alineado con el sistema integrado de gestión de Calidad, Medio Ambiente, Seguridad y Salud en el Trabajo de la Secretaría de Educación del Distrito.

1.3. FORMULACIÓN DEL PROBLEMA

¿Cómo el diseño del sistema de gestión de seguridad de la información, suministrará al Colegio Germán Arciniegas, herramientas que permitan fortalecer la seguridad, confidencialidad, disponibilidad e integridad de la información generada en la institución?

2. JUSTIFICACIÓN

De acuerdo con el informe de impactos de los incidentes de seguridad digital en Colombia 2017, la mayoría de las instituciones ya sean públicas o privadas no realizan restricciones a sus empleados para el acceso a Internet; por lo tanto es importante analizar y plantear medidas de protección que prevengan ser víctimas de ataques informáticos. Aunque muchas de las empresas colombianas aparentemente se encuentran preparadas para manejar un incidente no invierten en las áreas de organización de sus empresas para hacer frente a esto[13].

"En el caso de Colombia, el creciente uso de Tecnologías de la Información y las Comunicaciones (TIC), el aumento de conexiones a Internet, la masificación de las redes de telecomunicaciones como base para cualquier actividad socioeconómica y el incremento en la oferta de servicios disponibles en línea, evidencian un incremento significativo en la participación de los colombianos a través de canales electrónicos"[14], lo que hace necesario trabajar en los temas de seguridad.

Teniendo en cuenta que la información es uno de los activos más importantes al interior de una empresa, la información generada y tramitada en el Colegio Germán Arciniegas I.E.D. forma parte misional de la Secretaría de Educación del Distrito, por lo que se hace necesario el aseguramiento y estandarización de esta, mediante el diseño de un sistemas de gestión de seguridad de la información basado en las mejores prácticas que garanticen la integridad, conservación y organización de la información, donde el personal autorizado pueda consultar y acceder a ella de manera ordenada y administrar eficientemente los recursos informáticos.

La Secretaría de educación ha diseñado e implementado la Política de Seguridad de la Información en el cumplimiento de su misión con el fin de proteger, preservar y asegurar la integridad, confidencialidad y disponibilidad de los activos de información que soportan los procesos de la SED. En este sentido, las instituciones educativas como parte del nivel institucional de la SED, deben conocer e implementar esta política de seguridad para la protección de la información.

Teniendo en cuenta que la Secretaría de Educación cuenta en su nivel institucional con 362 instituciones educativas, en estas IED se maneja gran cantidad de información y sistemas informáticos, lo cual es importante contar con un sistema de gestión de seguridad de la información.

Con el diseño del SGSI para el colegio Germán Arciniegas, se busca el aprovechamiento de las TIC mediante un modelo de seguridad y privacidad de la

[13] Informe. Op. Cit., p. 14.
[14] Ibíd., p. 26.

información, se trabaja en el fortalecimiento de la seguridad de la información, la conservación, organización de la misma, garantizando la protección y la privacidad de los datos de los ciudadanos y funcionarios de la entidad mediante la identificación de los riesgos y el manejo adecuado de la gestión del riesgo todo esto acorde con lo expresado en la legislación Colombiana. Este SGSI será un referente para las instituciones educativas de la Secretaría de Educación.

El diseño del sistema de gestión de seguridad de la información SGSI bajo la norma técnica colombiana NTC-ISO-IEC 27001:2013, contará con los lineamientos para la implementación de este, que permitan que el colegio Germán Arciniegas se encuentre preparado frente a un incidente informático, un evento negativo o pérdida de la información y sea un referente para otras instituciones educativas.

En caso de que el sistema de gestión de seguridad de la información no se implemente en el Colegio Germán Arciniegas I.E.D., no se dará buen manejo a los riesgos y vulnerabilidades a los que se encuentra expuesta la institución y el impacto que se generaría en caso de materializarse una amenaza sería muy negativo.

3. ALCANCE Y LIMITACIONES

El diseño del sistema de gestión de la seguridad de la información que se realizará para el Colegio Germán Arciniegas I.E.D. bajo la norma técnica colombiana NTC-ISO-IEC 27001:2013, dentro del ciclo PHVA (planear, hacer, verificar y actuar) comprende solo fase de planeación del sistema no incluye la implementación, evaluación ni mejora. Este diseño se realizará a todas áreas y procesos internos del colegio Germán Arciniegas, no involucra la comunidad externa.

Para el diseño del SGSI del colegio Germán Arciniegas, se tendrán en cuenta las directrices dadas por la Secretaría de Educación del Distrito (SED) y los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones; dado que el colegio es una IED (institución educativa distrital) de carácter público que forma parte del nivel institucional de la Secretaría de Educación del Distrito, deberá cumplir con la normatividad que rigen a las entidades gubernamentales.

La Secretaría de Educación del Distrito cuenta con los niveles central, local e institucional y teniendo en cuenta que el colegio Germán Arciniegas pertenece al nivel institucional de la SED, el diseño del SGSI para la institución educativa estará articulado con el sistema integrado de gestión (SIG) de la Secretaría de Educación Distrital. El SIG de la Secretaría cuenta en el nivel central con los subsistemas de Gestión de la Calidad, Interno de Gestión Documental y Archivo, de Seguridad y Salud en el Trabajo, de Gestión de Seguridad de la Información, de Responsabilidad Social, de Gestión Ambiental y subsistema de Control Interno.

4. OBJETIVOS

4.1. OBJETIVO GENERAL

Diseñar el sistema de gestión de seguridad de la información, bajo la norma técnica colombiana NTC-ISO-IEC 27001:2013, para el Colegio Germán Arciniegas Institución Educativa Distrital (I.E.D.), que permita garantizar la confidencialidad, la disponibilidad e integridad de los datos.

4.2. OBJETIVOS ESPECÍFICOS

- Definir el contexto del colegio Germán Arciniegas, necesidades y expectativas de las partes interesadas.

- Determinar el alcance del sistema de gestión de seguridad de la información de la Institución Educativa Distrital.

- Valorar los riesgos a los que se encuentra expuesta la información del colegio y definir acciones para tratar riesgos y oportunidades.

- Definir los procesos y controles para la seguridad de la información que garanticen la disponibilidad, confiabilidad, e integridad de la información de la institución.

5. MARCO DE REFERENCIAL

5.1. MARCO TEÓRICO

El sistema de gestión es un conjunto ordenado de normas o procedimientos que interactúan entre sí, que mediante la ejecución de actividades coordinadas permita dirigir o administrar una organización, garantizando que determinada actividad se ejecute correctamente, buscando que las entidades sean eficaces logrando que lo planeado se cumpla.

Se entiende por información al conjunto de datos organizados, guardados, almacenados o transmitidos de diferentes maneras y que tienen gran valor en una organización o entidad; la seguridad de la información busca proteger y garantizar la confidencialidad, integridad y disponibilidad de la información.

"La seguridad de la información, consiste en la preservación de la confidencialidad, integridad y disponibilidad de la información, así como de los sistemas implicados en su tratamiento, dentro de una organización" [15]. Los conceptos de los atributos de la información como son confidencialidad, integridad y disponibilidad, se definen en la figura 1.

Figura 1 Conceptos de los atributos de la información.

Fuente el autor.

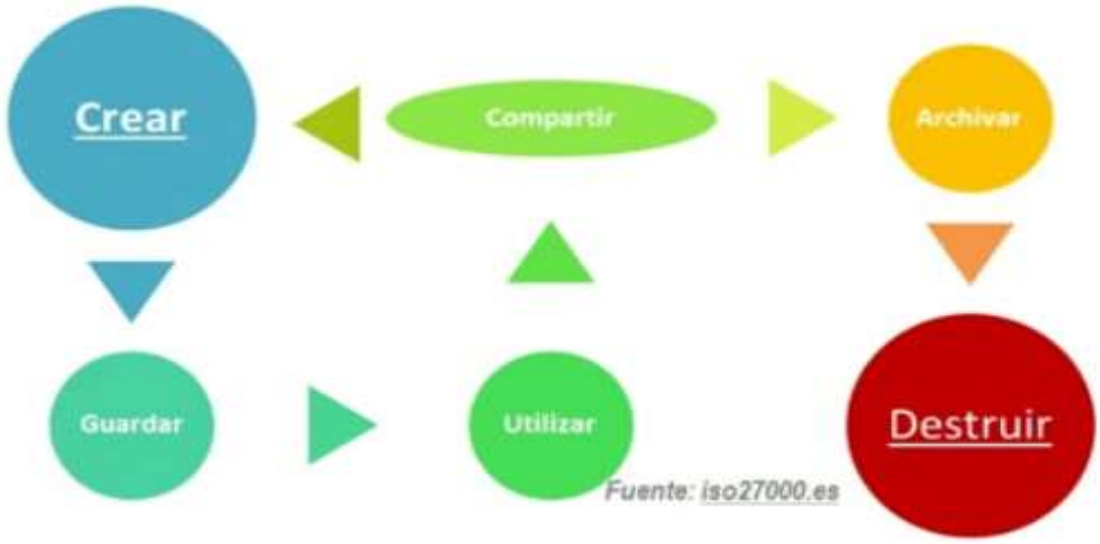
Con base al conocimiento del ciclo de vida de cada información, se debe adoptar el uso de un proceso sistemático el cual debe estar documentado, debe ser divulgado y conocido por la institución, desde un enfoque de riesgo empresarial.

[15] EL PORTAL DE ISO 27001 EN ESAPAÑOL. [en línea]. [Consultado 12 de marzo de 2018]. Disponible en http://www.iso27000.es/.

Este proceso es el que constituye el sistema de gestión de seguridad de la información[16].

El la figura 2 se describe el ciclo de vida de la información, la cual luego de creada, debe ser guardada en los diferentes medios de almacenamiento para luego ser utilizada, posteriormente se comparte lo que puede generar nueva información o la información estará lista para ser archiva o eliminada de acuerdo con la respectiva clasificación en las normas de archivo.

Figura 2. Ciclo de vida de la información



Fuente iso2700.es

No es posible garantizar un nivel de protección total, sin embargo, “el propósito de un sistema de gestión de la seguridad de la información es, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías”[17].

En algunos casos se confunde la seguridad de la información con la seguridad informática, la diferencia entre estas dos definiciones es que la seguridad informática protege los sistemas informáticos con el fin de asegurar la integridad y privacidad de la información que en estos se almacenan, mediante la implementación de técnicas y medidas que preserven las infraestructuras tecnológicas y de comunicación; a diferencia la seguridad de la información, no solo provee medidas de seguridad para los sistemas informáticos y la información almacenada en medios digitales, sino que va más allá en la protección de toda la

[16] Ibíd., p. 1.
[17] Ibíd., p. 1.

información de la empresa independiente del medio en que se encuentre almacenada.

Los sistemas de gestión establecen al interior de las organizaciones, estructuras que garantizan que una determinada actividad denominada gestión, se ejecute correctamente. La norma técnica colombiana NTC ISO IEC 27001 del año 2013, suministra los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información, con el fin de preservar la confidencialidad, la integridad y la disponibilidad de la información, mediante la gestión y tratamiento de los riesgos, que brinda confianza a las partes interesadas acerca de la gestión adecuada de los riesgos[18].

La NTC ISO/IEC 27001:2013, es la Norma Técnica Colombiana (NTC), publicado como tal por la International Organization for Standardization (ISO) y por la International Electrotechnical Commission (IEC), que organizaciones que se encargan de la estandarización de normas. En Colombia el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), es el organismo nacional de normalización, según el Decreto 2269 de 1993.

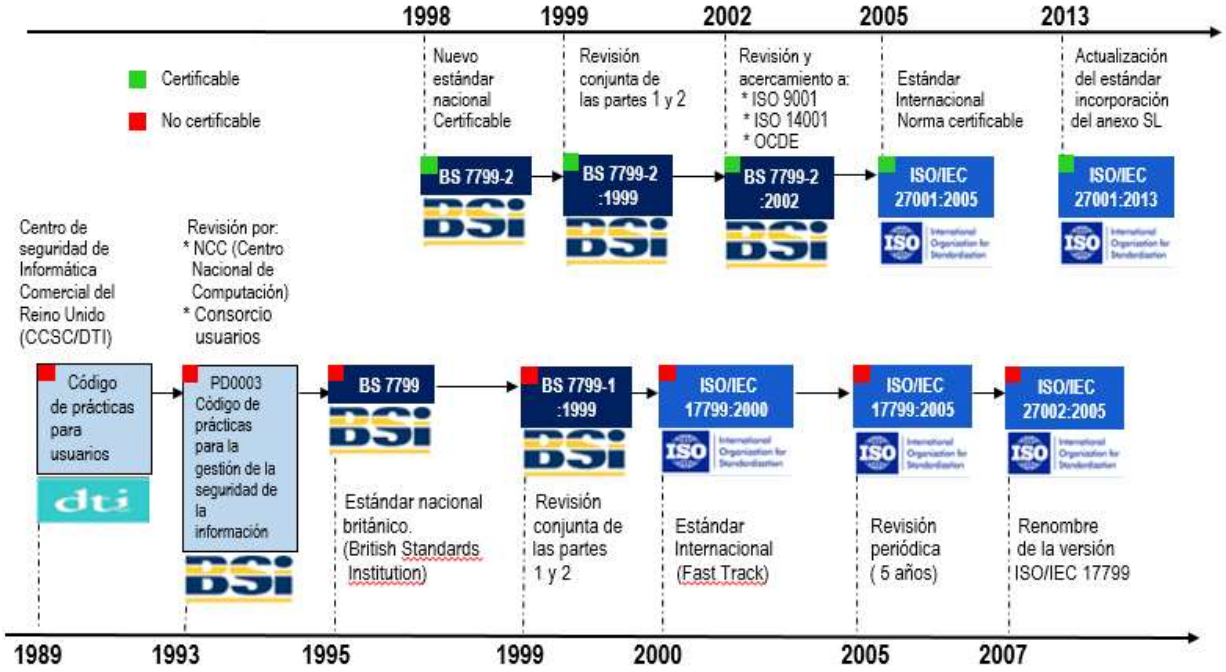
La estructura de la norma ISO 27001 versión 2005 cambio al pasar de 8 cláusulas a 10 en la versión 2013, la NTC ISO/IEC 27001:2013 está diseñada con el Anexo SL de las Directivas ISO/IEC la cual aplica la estructura de alto nivel, con títulos, numerales, idénticos, términos comunes que la hace compatible para su integración con otras normas de sistemas de gestión que han adoptado el Anexo SL, como son NTC ISO/IEC 9001:2015 NTC ISO/IEC 14001:2015[19].

La primera publicación de la norma ISO/IEC 27001 fue en el año 2005, posteriormente se realizan alguna modificaciones las cuales se publicaron en el año 2013 y es la versión que actualmente se utiliza para el diseño, implementación, control y seguimiento del Sistema de Gestión de Seguridad de la Información; sin embargo esta norma puede ser actualizada periódicamente para que responda a las necesidades y exigencias de la actualidad.

Esta norma que actualmente se conoce, ha sido resultado de la evolución de otros estándares relacionados con la seguridad de la información, donde inicia en el año 1989 con el código de prácticas de usuarios que posteriormente se modificó como el código de prácticas para la gestión de la seguridad de la información hasta llegar a ser la primer versión de ISO/IEC 27001 como se evidencia en la figura 3.

[18] INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Sistemas de gestión de la seguridad de la Información: técnicas de seguridad y requisitos. NTC-ISO/IEC 27001. Bogotá D.C.: El Instituto, 2013. i p.
[19] Ibíd., p. i.

Figura 3. Historia de ISO 27001 e ISO 17799



Fuente el autor

La norma ISO/IEC 27001:2005 fue la primera versión de esta norma, posteriormente se adoptaron los requisitos especificados en la nueva publicación ISO/IEC 27001:2013 que reduce esfuerzos en cuestiones relevantes como son la aplicación de metodologías de análisis del riesgo, la mejora continua y la eliminación del enfoque a procesos.

5.1.1. Breve historia de las TIC en Colombia

El 14 de mayo de 1514 se creó el correo mayor de indias, mediante privilegio que concedió la Corona Española a don Lorenzo Galíndez de Carvajal. La Casa Real Administración de Correos fue construida desde 1553 en la esquina sur de la catedral de Bogotá[20].

En 1937 abrió operaciones en Bogotá la empresa Watson Business Machines Co. of Colombia, cuyo objeto era la comercialización de relojes, balanzas, máquinas

[20] Ministerio de Tecnologías de la Información y las Comunicaciones. Gobierno de Colombia. [en línea]. Historia. Colombia. (26 de febrero de 2018). Disponible en http://www.mintic.gov.co/portal/604/w3-propertyvalue-6077.html

de escribir y equipos de tabulación y que hoy se conoce con el nombre de IBM[21] y el 3 de marzo de 1957 llega el primer computador a Colombia[22].

En el gobierno de Manuel Murillo Toro se envió el primer mensaje telegráfico de la historia colombiana entre el municipio de Cuatro Esquinas Mosquera y la Capital de la República, el primero de noviembre de 1865 realizado por el ingeniero William Lee Stiles y el mensaje estaba dirigido al presidente[23]. En 1913, la empresa Marconi Wireless empezó a prestar el servicio de telegrafía en el país con una red compuesta por doce ciudades.

A través de la red BITNET de IBM, con los esfuerzos de algunas universidades del país, y el apoyo del Instituto Colombiano de Fomento para la Educación Superior, ICFES y la Compañía Colombiana de Telecomunicaciones TELECOM, en 1991 se logra conectar un canal análogo entre la Universidad de Columbia en New York y la Universidad de los Andes en Bogotá. RUNCOL se llamó a la red de Universidades Colombianas que contaba con la participación de más de 30 universidades del país. RUNCOL sólo brindaba el uso del correo electrónico a través del protocolo de comunicación NJE, manejado por la red BITNET de IBM[24].

El 17 de junio de 1991 se registra el primer dominio .co por parte de la Universidad de los Andes y el 14 de mayo de 1994 esta universidad lanza su página web, que sería la primera del país. En 1998 Asobancaria implementa por primera vez la posibilidad de realizar pagos a través de internet, en el 2000 Colombia recibió oficialmente la banda ancha a través de una conexión de fibra óptica y en 2008 Colombia inicia el uso de internet móvil mediante operadores de telefonía celular[25].

5.1.2. Breve historia de los hackers

Según Cano (2015, p.39), "*se podría decir que los hackers son los constructores del manual de lo "no documentado", de la realidad que está inmersa en las soluciones de informática que aún no se descubre o se escribe para que otros la*

[21] Portafolio. Finanzas. [en línea]. IBM Colombia siete décadas de innovación. Colombia. (30 de octubre de 2007). Disponible en http://www.portafolio.co/economia/finanzas/ibm-colombia-siete-decadas-innovacion-llegada-compania-ofrecio-pais-relojes-balanzas-maquinas-escribir-tabulacion-386158

[22] Semana. Tendencias. [en línea]. La máquina que cambió al país. Colombia. (30 de octubre de 2007). Disponible en https://www.semana.com/especiales/articulo/marzo-1957-brla-maquina-cambio-pais/65917-3

[23] El tiempo. Archivo. [en línea]. Así fue la primera comunicación telegráfica. Colombia. (1 de noviembre de 1995). Disponible en http://www.eltiempo.com/archivo/documento/MAM-442432

[24] Diario el amanecer. Herramientas educativas para generar recursos digitales. [en línea]. Historia de Internet en el mundo y su llegada a Colombia. Colombia. (marzo de 2015). Disponible en http://es.calameo.com/read/0042539398be5661ee9aa.

[25] ANA Arbeláez. Enter.co. [en línea]. 19 datos que usted no sabía sobre internet en Colombia. Colombia. (16 de mayo de 2014). Disponible en http://www.enter.co/cultura-digital/colombia-digital/19-datos-que-usted-no-sabia-sobre-internet-en-colombia/.

observen. El movimiento hacking es y será una fuerza motriz del desarrollo de mejoras en el mundo del software"[26].

El hacking inicia a finales de los años 50 con el manejo de la máquina TX-0 en el Instituto Tecnológico de Massachusetts conocido como MIT por sus siglas en inglés. Con el avance tecnológico aparece el primer computador producido en serie Programmed Data Processor-1 conocido como PDP, donde se jugó el primer videojuego de la historia el Spacewar de Steven Russell. Posteriormente se desarrolló toda una generación de PDP hasta contar con el PDP-11 que fue el más exitoso, ya que contaba con un sistema integrado[27].

A finales de los años 60 y principio de los 70, a causa de la guerra y a la defensa ante un ataque nuclear, se desarrollan nuevas estrategias de comunicación, redes y computación. ARPA (Advanced Research Project Agency) coordinaba esta iniciativa de defensa donde se crea la red Arpanet que posteriormente se convierte en lo que se conoce como Internet. Entre 1970 y 1980 surgen nuevos desarrollos como nuevos procesadores, aplicaciones, avances en redes, bases de datos relacionales, sistemas de procesamiento compartido, estrategias de seguridad de la información entre otros[28].

Al inicio de los 80 Vinton Cerf y Robert Kahn hacen posible la red más grande de computadoras interconectadas a nivel mundial mediante los protocolos TCP/IP. Se dispone del sistema operativo UNIX, se desarrollan lenguajes de programación, se dispone de herramientas como depuradores y compiladores; en 1989 Tim-Berneers Lee, estableció la comunicación entre cliente y servidor mediante el protocolo HTTP y creó la World Wide Web (www) tecnología en la que se fundamenta la web.

Aunque es hasta 1984 cuando se adopta el término de virus informático, en 1972 se materializó una amenaza de un programa llamado creeper (enredadera), que aparecía en la pantalla del equipo afectado de manera aleatoria. Con los avances a finales de los 80, se generó una lucha por el control de territorios informáticos y el termino hacker pasó de ser un título positivo que se ganaba por sus méritos y logros a un título negativo asociado con vándalo o intruso informático[29].

[26] CANO MARTÍNEZ, Jeimy José. Computación Forense: descubriendo los rastros informáticos. 2 ed. Bogotá: Alfaomega Colombiana S.A. 2015. 271 p. ISBN 978-958-682-922-9.
[27] Ibíd., p. 40.
[28] Ibíd., p. 41.
[29] Ibíd., p. 43.

5.1.3. Gobierno digital

Dado que los avances tecnológicos van en creciente aumento, así como las aplicaciones, la comunicación y los sistemas de información; en Colombia se han implementado el uso de los recursos tecnológicos a través del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), gobierno se encarga de promover el uso de las Tecnologías de la Información y las Comunicaciones.

En la Ley 1712 del 6 de marzo de 2017, por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones, en su artículo 3 se determinan los principios de la transparencia y acceso a la información pública; entre estos principios está el principio de la divulgación proactiva de la información[30].

Los actores fundamentales para el desarrollo integral del Gobierno Digital en Colombia son el Estado y la sociedad, donde las necesidades, y problemáticas determinan el uso de la tecnología mediante un entorno de confianza digital que sea sencillo, amigable y seguro, en donde se relaciona el Estado con los ciudadanos actores del ecosistema digital.

En la implementación de la Política de Gobierno Digital, donde se propone el uso y aprovechamiento de las TIC mediante servicios digitales de confianza, el desarrollo de procesos internos eficientes, la toma de decisiones basadas en datos, el empoderamiento ciudadano y el impulso en el desarrollo de territorios y ciudades inteligentes, intervienen varios elementos que brindan orientaciones que deben ser acogidas por las entidades, como son los componentes TIC para el Estado y TIC para la Sociedad que mediante los tres habilitadores transversales Arquitectura, Seguridad y privacidad y Servicios Ciudadanos Digitales, son los elementos de base que permiten el desarrollo de los componentes de la política.

[30] CONGRESO DE LA REPÚBLICA. Ley 1712. (6, marzo, 2014). Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones. Bogotá D.C. El Congreso. 2014. 14 p. Disponible en: http://www.mintic.gov.co/portal/604/articles-7147_documento.pdf

Figura 4. Elementos que intervienen en la política de gobierno digital.

Fuente http://www.mintic.gov.co/portal/604/w3-article-61775.html

El Ministerio de las telecomunicaciones ha creado la Arquitectura TI, con la cual busca unir los esfuerzos de entidades públicas para ser más eficiente, se basa en el Marco de Referencia como instrumento principal que establece la estructura conceptual, define lineamientos e incorpora mejores prácticas y traza la ruta de implementación de la Arquitectura TI. Adicionalmente habilitar la estrategia de Gobierno en línea compuesta por TIC para servicios, TIC para la gestión, TIC para el gobierno abierto y para la seguridad y la privacidad.

La misión de las instituciones es servir a los ciudadanos de manera transparente, con servicios y trámites ágiles y efectivos, con información precisa y de alta calidad en los procesos públicos. Para esto Colombia está fortaleciendo sus entidades públicas a través del Ministerio de las TIC, con el diseño e implementación de la política de Gobierno Digital antes conocida como la Estrategia de Gobierno en línea, soportada en la construcción de la Arquitectura TI del Estado y el modelo de gestión estratégica con TI; con el fin de organizar y promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado participativo, eficiente y transparente.

5.2. MARCO CONCEPTUAL

5.2.1. Gestión del riesgo

El riesgo es esa vulnerabilidad o amenaza a que ocurra un evento negativo y que algo o alguien puedan verse afectados por él. También es considerado como la exposición de una situación donde hay una posibilidad de sufrir un daño o de estar en peligro. El riesgo y peligro se diferencian ya que el peligro es la condición o característica que puede causar un daño o lesión y el riesgo es la combinación entre la probabilidad de ocurrencia del evento y la consecuencia de no controlar el peligro. La gestión del riesgo hace referencia al proceso para mantener un

ambiente seguro y crear medidas que permitan dar un tratamiento eficaz del riesgo disminuyendo el impacto negativo.

Los activos a nivel tecnológico son todos aquellos elementos relacionados con los sistemas de información, las redes, comunicaciones y la información en sí misma. Es importante identificar no solo los riesgos de los activos sino también las vulnerabilidades, amenazas e impactos

La seguridad informática, se encarga de la identificación de las vulnerabilidades del sistema, del establecimiento de controles y medidas que eviten que las distintas amenazas posibles se materialicen en dichas vulnerabilidades y generen un alto impacto negativo. La vulnerabilidad hace referencia a la debilidad o grado de exposición de un sujeto, objeto o sistema, es el punto o aspecto susceptible de ser atacado o de dañar la seguridad del mismo, representan las debilidades en el sistema informático. En la tabla 2, se describen algunos tipos de vulnerabilidades[31].

Tabla 2. Tipos de vulnerabilidades.

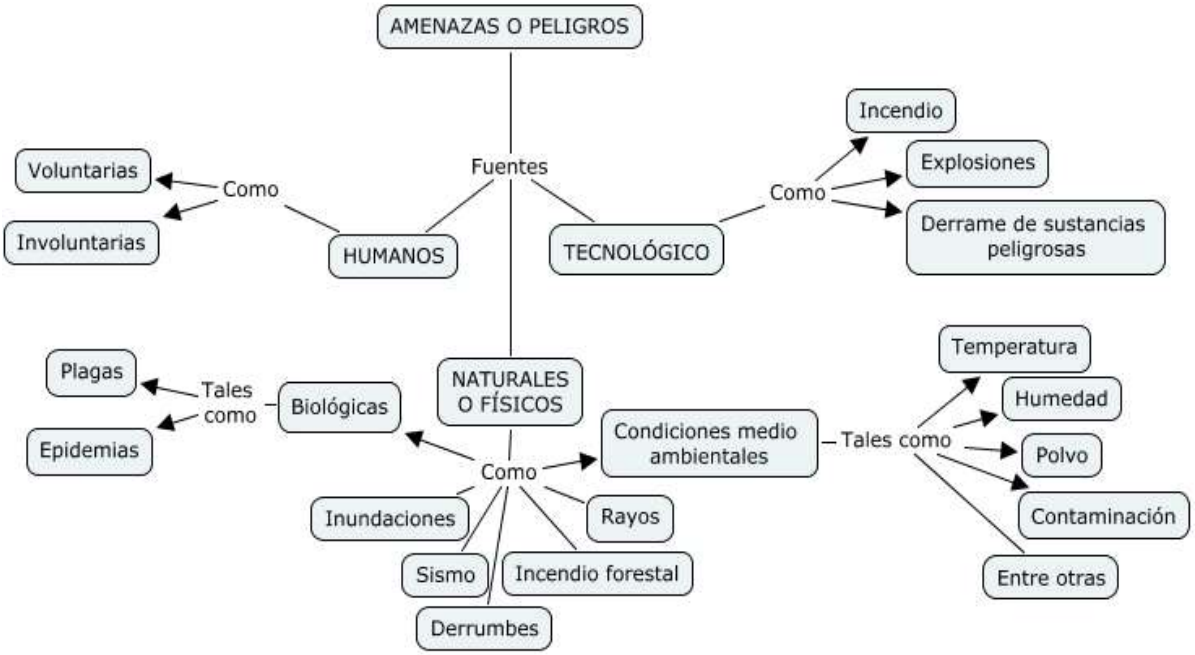
Vulnerabilidad	Descripción
Física	Es la posibilidad de acceder al sistema directamente desde el equipo, para extraerle información, alterarlo o destruirlo.
Natural	Es la posibilidad de que el sistema sufra daños por causas del ambiente o desastres naturales, como incendios, tormentas, inundaciones, terremotos, humedad excesiva, picos de bajas y altas temperaturas.
Emanación	Es la posibilidad de interceptar radiaciones electromagnéticas para descifrar o alterar la información enviada y recibida.
Software	También conocida como bugs, es la posibilidad de que el sistema sea accesible debido a fallas en el diseño del software.
Comunicaciones	Es la posibilidad de que varios usuarios puedan acceder a un sistema informático que se encuentra conectado a una red de computadoras o una red global (internet).
Humana	La posibilidad del error humano. Los administradores y usuarios del sistema son una vulnerabilidad, ya que tienen acceso a la red y al equipo.

Fuente https://capacitateparaelempleo.org/assets/4aq4l6q.pdf.

La amenaza es la probabilidad de ocurrencia de un suceso negativo o destructivo; se refiere a un peligro latente o factor de riesgo de un sistema o de un sujeto expuesto. Una amenaza informática es un posible peligro del sistema. Puede ser una persona, un programa, o un suceso natural o de otra índole. Las amenazas informáticas están representadas en los posibles atacantes o factores que aprovechan las debilidades del sistema. A continuación en la figura 5, se describe la clasificación de las amenazas.

[31] FUNDACION CARLO JLIM. Vulnerabilidades informáticas. [En línea]. Disponible en: https://capacitateparaelempleo.org/assets/4aq4l6q.pdf

Figura 5. Clasificación de las amenazas.



Fuente el autor.

Debido a la variedad de amenazas hay tres aspectos que se ven en riesgo, que son el hardware, el software y los datos. Las amenazas causadas por la fuente humana y de manera voluntaria se conocen como ataques y a continuación en la tabla 3, se describen algunos de los ataques más realizados:

Tabla 3. Descripción de ataques más realizados.

Ataque	Descripción
Ataques DDoS	DDoS son las siglas de Distributed Denial of Service. La traducción es "ataque distribuido denegación de servicio", y traducido de nuevo significa que se ataca al servidor desde muchos ordenadores para que deje de funcionar.
Adware	Su nombre se deriva de la combinación de las palabras ADvertisement (anuncio) y softWARE, consiste en un programa malicioso que se instala en el computador sin que el usuario lo note, y cuya función es descargar y mostrar anuncios publicitarios en la pantalla de la víctima, no produce una modificación explícita que dañe el sistema operativo, pero sí disminuye el rendimiento del equipo y de la navegación por la red ya que utiliza recursos del procesador, la memoria y el ancho de banda.
Backdoor o puerta trasera	En ocasiones, algunos programadores maliciosos dejan una puerta trasera para así poder evitar los sistemas de seguridad de acceso para poder acceder al sistema con total comodidad y sin conocimiento de los usuarios.
Botnets	Es una red de equipos infectados (robot o zombi) por códigos maliciosos, los cuales son controlados por un delincuente informático quien de manera remota envía órdenes a los equipos zombis haciendo uso de sus recursos. Las acciones de un equipo zombi son realizadas en su totalidad de forma transparente al

Ataque	Descripción
	usuario. Por este motivo, uno de los síntomas más importantes de un sistema infectado por un malware de este tipo es el consumo excesivo de recursos, el cual hace lento el funcionamiento del sistema y de las conexiones, e incluso puede llegar a impedir su utilización.
Gusanos	Es un tipo de virus informático que tiene la propiedad de duplicarse a sí mismo, una diferencia con los virus tradicionales es que no necesitan de un archivo anfitrión para seguir vivos, por lo que se reproducen utilizando diferentes medios como las redes locales o el correo electrónico; otra diferencia es que su objetivo no es necesariamente provocar un daño al sistema, sino copiarse a la mayor cantidad de equipos como sea posible o en otros casos, simplemente intentan agotar los recursos del sistema como memoria o ancho de banda mientras intenta distribuirse e infectar más ordenadores.
Hacker	Un hacker en la informática es conocido como un usuario ajeno que entra en tu computadora con intenciones de robar información y de causar daño (al igual que un spyware) con la diferencia es que en este caso hablamos de una persona física que a través de sus conocimientos rompe las barreras que se les interpongan para entrar a un sitio o una computadora.
Ingeniería social	Es una acción o conducta social destinada a conseguir información de las personas cercanas a un sistema por medio de habilidades sociales. Con esto se busca que el usuario comprometa al sistema y revele información valiosa por medio de variados tipos de engaños.
Malware	Es el acrónimo, en inglés, de las palabras 'malicious' y 'software', por lo que se conoce como software malicioso, cuyo objetivo es el de variar el funcionamiento de cualquier sistema informático sin que el usuario infectado lo note.
Pharming	Redirecciona con mala intención al usuario a un sitio web falso mediante la explotación del sistema DNS, denominándose secuestro o envenenamiento del DNS.
Phishing	Consiste en el robo de información personal y financiera del usuario, a través de la falsificación de un ente de confianza. El usuario recibe un correo electrónico simulando la identidad de una organización de confianza, por lo que este, al confiar en el remitente, envía sus datos directamente al atacante.
Ransomware	Es un programa que bloquea el equipo afectado, con un mensaje en el que se pide un rescate para que el usuario pueda volver a recuperar el control. Se le exige un rescate en Bitcoin para que no pueda ser rastreada la persona o personas que han lanzado esta amenaza.
Rootkit	Son herramientas como programas, archivos, procesos, puertos o cualquier componente lógico diseñadas para mantener en forma encubierta el control de un computador. No es un software maligno en sí, sino que permite ocultar las acciones malignas que se desarrollan en un equipo.
Scam	Es el nombre utilizado para las estafas a través de medios tecnológicos. Los medios utilizados por el scam son similares a los que utiliza el phishing, si bien su objetivo no es obtener datos sino lucrar de forma directa a través del engaño. Las técnicas más comunes son el anuncio de una ganancia extraordinaria o las peticiones de ayuda caritativa.
Spam	Todo correo no deseado recibido por el destinatario, el cual viene de un envío automático y masivo por parte de aquel que lo emite, generalmente se asocia al correo electrónico personal, pero no sólo afecta a los correos electrónicos personales, sino también a foros, blogs y grupos de noticias.
Spyware	Se trata de un programa espía que tiene la capacidad de recopilar información de un computador y transmitirla sin el conocimiento de la persona afectada, poniendo en peligro la seguridad del equipo afectado (claves, cuentas de correo, cuentas bancarias, etc.).

Ataque	Descripción
Trashing	Consiste en rastrear en las papeleras en busca de información, contraseñas o directorios, aunque con la explosión de Internet parece estar un poco de capa caída, al menos no se escucha tanto, en su día el Trashing, o el buscar Información en los cubos de basura de las empresas, era una técnica común.
Troyanos	Su nombre proviene de la leyenda del caballo de Troya, pues se disfraza para engañar al usuario. En este caso, se trata de un programa que cuando se ejecuta, proporciona al atacante la capacidad de controlar el equipo infectado de forma remota y en muchas ocasiones sin el conocimiento del usuario.
Virus informático	Es un programa que se copia automáticamente y que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus son programas que se replican y ejecutan por sí mismos. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este.

Fuente el autor.

Los impactos son las consecuencias de la ocurrencia de una o varias amenazas y los daños por pérdidas que éstas puedan causar. Dependiendo de la magnitud del impacto, la pérdidas pueden ser altas, medias o bajas; estas pérdidas pueden ser financiaras, económicas, tecnológicas, físicas, humanas, entre otras.

5.2.2. Metodologías de análisis del riesgo

En un SGSI es importante establecer una metodología de análisis de riesgos que permita dar a conocer las debilidades y fortalezas con que cuenta la organización, valorar los procesos más críticos, determinar y evaluar las amenazas, evaluar el nivel de protección, planificar las medidas necesarias para reducir los impactos. Para realizar un efectivo análisis de riesgos, en la seguridad de la información existen diversas metodologías, entre las más reconocidas se tienen Octave, Fair, ISO 27005, TARA, Magerit, Mehari, NIST SP 800:30, Estándar COSO, Estándar COBIT, Coras, Cramm y Ebios[32].

En la metodología Margerit, se define los siguientes pasos en el análisis de riesgos:

- Determinar los activos importantes para la institución.
- Determinar las amenazas están expuestos aquellos activos.
- Determinar qué salvaguardas hay dispuestas y su eficacia.
- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.

[32] ALEMÁN NOVOA, Helena y RODRÍGUEZ BARRERA, Claudia. Metodologías Para el Análisis de Riesgos en los SGSI. [En línea]. 2015. Vol. 9. Disponible en http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia de la amenaza.

No todas las amenazas afectan todos los activos y en algunos casos el activo no se ve afectado en todas sus dimensiones por la amenaza. Una vez se determine que una amenaza puede afectar un activo, hay que valorar el grado en que se afecta el activo, que puede ser por degradación que hace referencia al daño causado al valor del activo y por probabilidad que es la probabilidad que se tenga de la materialización de la amenaza.

A continuación en la tabla 4, se realiza la escala de medición por la degradación del activo y en la tabla 5, se presenta la medición de la probabilidad que se materialice la amenaza.

Tabla 4. Medición por degradación.

MA	100%	Muy alta	Daño muy grave
A	75%	Alta	Daño grave
M	50%	Media	Daño importante
B	25%	Baja	Daño menor
MB	1%	Muy Baja	Daño despreciable

Fuente: MAGERIT versión 3.0. Metodología de Análisis y Gestión de Riesgos

Tabla 5. Medición por degradación.

MA	100	Muy frecuente	A diario
A	10	Frecuente	Mensualmente
M	1	Normal	Una vez al año
B	1/10	Poco frecuente	Cada varios años
MB	1/100	Muy poco frecuente	Siglos

Fuente: MAGERIT versión 3.0. Metodología de Análisis y Gestión de Riesgos

Para determinar del impacto potencial una vez materializada la amenaza, se calcula el impacto del daño sobre el activo teniendo en cuenta su valor y su degradación, así:

$$\text{Impacto} = \text{Valor} \times \text{Degradación}$$

Para determinar el riesgo potencial, se evalúa el riesgo en función del impacto y su probabilidad de ocurrencia, como se describe en la fórmula a continuación:

$$\text{Riesgo} = \text{Impacto} \times \text{Probabilidad}$$

5.2.3. Salvaguardas

Las salvaguardas se definen como aquellos procedimientos o mecanismos que reducen el riesgo, son elementos de defensa que disminuye la probabilidad de materializarse una amenaza y limita el daño. Existen diferentes tipos de protección, como se relacionan en la tabla 6.

Tabla 6. Tipos de salvaguardas.

Efecto	Tipo
Preventivas: reducen la probabilidad	[PR] preventivas [DR] disuasorias [EL] eliminatorias
Acotan la degradación	[IM] minimizadoras [CR] correctivas [RC] recuperativas
Consolidan el efecto de las demás	[MN] de monitorización [DC] de detección [AW] de concienciación [AD] administrativas

Fuente MAGERIT versión 3.0. Metodología de Análisis y Gestión de Riesgos

Las salvaguardas se caracterizan por su eficacia frente al riesgo. Una eficacia del 100% son para aquellas que son idóneas y están perfectamente implantadas, una eficacia del 0%, son para aquellas que falta. Se puede emplear una escala de madurez que mida la confianza de la salvaguarda en el proceso de la gestión como se describe en la tabla 7.

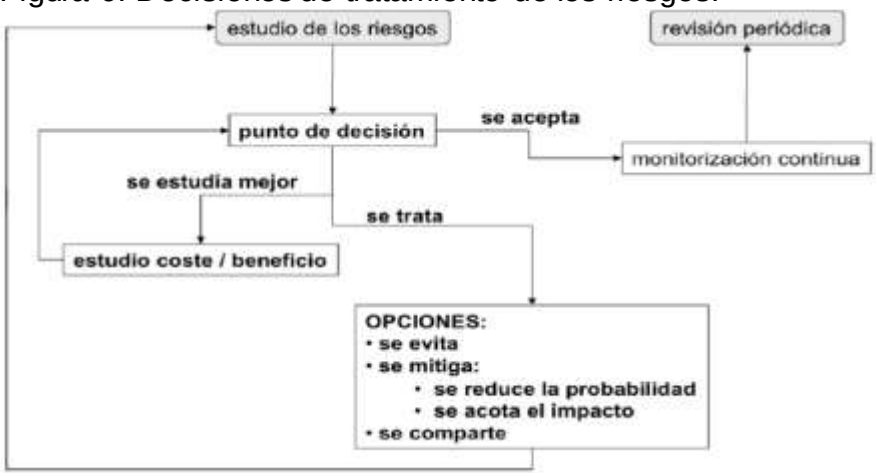
Tabla 7. Valoración de salvaguarda0073.

Factor	Nivel	Significado
0%	L0	Inexistente
	L1	Inicial / ad hoc
	L2	reproducible, pero intuitivo
	L3	proceso definido
	L4	gestionado y medible
100%	L5	optimizado

Fuente MAGERIT versión 3.0. Metodología de Análisis y Gestión de Riesgos

El resultado del análisis es sólo un análisis de los riesgos, permite a partir de los resultados tomar decisiones conociendo lo que se quiere proteger y las medidas tomadas para por protegerlo (salvaguardas valoradas). Todo ello sintetizado en los valores de impacto y riesgo. En la figura 6, se evidencia las posibles decisiones del tratamiento que se pueden tomar, luego de realizar el estudiado de los riesgos.

Figura 6. Decisiones de tratamiento de los riesgos.



Fuente MAGERIT versión 3.0. Metodología de Análisis y Gestión de Riesgos

5.3. MARCO LEGAL

Para el desarrollo del Sistema de gestión de seguridad de la información del Colegio Germán Arciniegas I.E.D., se ha tenido en cuenta toda la legislación existente en Colombia que se encuentre relacionada con la seguridad de la información.

Decreto 1078 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones el 26 de mayo de 2015, donde dispone que las entidades que conforman la administración pública serán sujetos obligados al cumplimiento de las políticas y los lineamientos de la Estrategia de Gobierno en Línea y estableció como uno de sus cuatro componentes el de la seguridad y privacidad de la información comprendido por las acciones trasversales a los componentes de TIC para Servicios, TIC para el Gobierno Abierto y TIC para la Gestión, tendientes a proteger la información y sistemas de información, del acceso, divulgación, interrupción o destrucción no autorizada.

Decreto 2578 de 2012, por el cual se reglamenta el Sistema Nacional de Archivos, se establece la Red Nacional de Archivos, se deroga el Decreto 4124 de 2004 y se dictan otras disposiciones relativas a la administración de los archivos del Estado. Emitido por el Ministerio de Cultura el 13 de diciembre de 2012.

Documento CONPES 3701 (Consejo Nacional de Política Económica y Social) del 14 de julio de 2011, contiene los lineamientos de política para ciberseguridad y ciberdefensa. El Gobierno Nacional a través de este documento estableció la estrategia nacional de ciberseguridad y ciberdefensa, con el fin de desarrollar

medidas que aseguren la información de los ciudadanos frente a las amenazas informáticas y que deben ser adoptados.

Ley 527 de 1999, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. El Congreso de la República de Colombia emite esta ley el 18 de agosto de 1990, esta se modifica con el Decreto 2364 del 22 de noviembre del 2012, por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.

Ley 594 de 2000, por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones. El Congreso de la República de Colombia emite esta ley el 14 de julio de 2000.

Ley 1266 de 2008, por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. El Congreso de la República de Colombia emite esta Ley el 31 de diciembre de 2008.

Ley 1273 de 2009, Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. El Congreso de la República de Colombia emite esta ley el del 5 de enero de 2009, conocida también como la ley de los delitos informáticos.

Ley 1341 de 2009, por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. El Congreso de Colombia emite esta el 30 de julio.

Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales. El Congreso de la República de Colombia emite esta ley el 17 de octubre de 2012 y reglamentada parcialmente por el Decreto Nacional 1377 de 2013.

Ley 1712 de 2014, por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones. El Congreso de la República de Colombia emite esta ley el 6 de marzo de 2014.

Resolución 1944 del 27 de octubre de 2016, de la secretaría de Educación del Distrito, por medio de la cual se adopta la Política de Seguridad de la Información

de la Secretaría de Educación del Distrito, donde se establecen los objetivos de la y lineamientos de la política.

Resolución 1945 del 27 de octubre de 2016, de la secretaría de Educación del Distrito, por medio de la cual se crea el Comité Técnico del Subsistema de Seguridad de la Información de la Secretaría de Educación del Distrito y se definen los roles y responsabilidades.

Resolución 305 del 20 de octubre de 2008 de la Comisión Distrital de Sistemas de Bogotá D.C., por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.

Resolución 3313 del 18 de diciembre de 2017 del Ministerio de Tecnologías de la Información y las Comunicaciones, por la cual se actualiza el plan vive digital 2014-2018 contenido en el anexo de la Resolución 828 del 11 de mayo de 2015 y se deroga la Resolución 1564 de 2016.

6. DISEÑO METODOLÓGICO

6.1. TIPO DE INVESTIGACIÓN

El enfoque de la investigación para el diseño del sistema de gestión de seguridad de la información en el Colegio Germán Arciniegas es mixto, teniendo en cuenta la aplicación de herramientas que permitan valorar la gestión del riesgo, gestión documental, gestión de incidentes, controles de seguridad e indicadores de gestión que permitan un análisis de impactos, evaluación de desempeños para la toma de decisiones en la mejora continua.

El diseño del SGSI para el colegio Germán Arciniegas cuenta con los tipos de investigación descriptiva y explicativa. Descriptiva porque en el presente documento se describe el estado actual de la seguridad de la información en la institución educativa, se realiza la recolección de datos con el fin de analizarlos y formular hipótesis para la toma de decisiones; y explicativa, porque con la información recolectada se define el ¿por qué? y el ¿para qué? del sistema de gestión de seguridad informática

6.2. FUENTES DE INFORMACIÓN

6.2.1. Fuentes de información primaria

La información recolectada es suministrada por el personal de la institución educativa distrital, conformado por los profesores, directivos, orientadores, personal de apoyo y administrativo.

6.2.2. Fuentes de información secundaria

El diseño del sistema de gestión de seguridad de la información para el colegio Germán Arciniegas se basa en la norma técnica colombiana NTC-ISO-IEC 27001:2013, adicionalmente se tendrán en cuenta las guías del modelo de seguridad, suministradas por el MINTIC:

- ⇨ Modelo de seguridad y privacidad de la información.
- ⇨ Metodológica de Pruebas de Efectividad.
- ⇨ Elaboración de la política general de seguridad y privacidad de la información.
- ⇨ Procedimientos de seguridad de la información
- ⇨ Roles y Responsabilidades
- ⇨ Gestión y Clasificación de Activos de Información.
- ⇨ Referencia sobre Gestión Documental
- ⇨ Gestión de riesgos

- ⇨ Controles de Seguridad y Privacidad de la Información
- ⇨ Indicadores de gestión para la seguridad de la información
- ⇨ Análisis de Impacto
- ⇨ Seguridad en la Nube
- ⇨ Plan de Capacitación, Sensibilización Y Comunicación De Seguridad De La Información
- ⇨ Auditorías
- ⇨ Mejora continua
- ⇨ Gestión y Clasificación de Incidentes de Seguridad de la Información.
- ⇨ Pacto de Convivencia 2018 y del Sistema Institucional de Evaluación Escolar (SIEE) 2018 del Colegio Germán Arciniegas I.E.D.

6.3. POBLACIÓN Y MUESTRA

Para la recolección de la información que permita el diseño del SGSI en el Colegio Germán Arciniegas, se cuenta con una población grande teniendo como criterio +50, para la recolección de la información. Esta población es el personal de la institución educativa distrital, conformado por los profesores, directivos, orientadores, personal de apoyo y administrativo. En la tabla 8, se detalla la cantidad de la población para la recolección de la información.

Tabla 8. Cantidad de la población.

Personal	Cantidad
Profesores	70
Directivos docentes	5
Orientadores	5
Docentes de apoyo	3
Personal administrativo	5
Total	88

Fuente el autor.

6.4. INSTRUMENTOS Y TÉNICAS DE RECOLECCIÓN DE INFORMACIÓN

Para la recolección de la información se tendrán en cuenta los siguientes instrumentos:

- ➢ Encuesta dirigida al personal interno de la institución, diseñada en un formulario web, consta de 17 preguntas abiertas.

- ➢ A los docentes jefes de áreas, un representante de los directivos docentes, un representante de los orientadores, un representante del docentes de apoyo y personal administrativo, se les aplica la encuesta diagnóstico del estado de la seguridad de la información en la Institución educativa, como

base se toma el Anexo A de Norma Técnica Colombiana ISO-IEC 27001 del 2013, que consta de 70 preguntas cerradas.

- La norma técnica colombiana NTC-ISO-IEC 27001:2013 es el instrumento guía para el desarrollo del diseño del Sistema de Gestión de Seguridad de la Información para el Colegio Germán Arciniegas IED, con apoyo de las directrices dadas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) en el modelo de seguridad, disponible en su página web http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html.

6.5. TÉCNICAS DE ANÁLISIS DE LA INFORMACIÓN

Las encuestas aplicadas al personal de la institución serán tabuladas en Excel y representadas gráficamente, para el respectivo análisis descriptivo. De acuerdo con los resultados obtenidos, se validará la información para la evaluación de los riesgos y los respectivos niveles de impacto de acuerdo con las escalas establecidas en la metodología de análisis y gestión de riesgos.

7. DISEÑO DEL SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

7.1. CONTEXTO DE LA ORGANIZACIÓN

7.1.1. Conocimiento de la organización y de su contexto

Reseña histórica del colegio Germán Arciniegas I.E.D.

En el año 2007 el colegio Germán Arciniegas surgió con el nombre de Brasil López Quintana producto de la ampliación de la cobertura asumida por el colegio oficial Brasilia.

Los testimonios de los docentes que asumieron las labores educativas en esta época reflejan las dificultades que se tuvieron que vivir en los primeros años de vida del colegio:

> "Durante los primeros dos meses los estudiantes de bachillerato del Brasil López Quintana fueron ubicados en algunos espacios de la sede A del colegio Brasilia, desarrollando su proceso escolar en jornadas de emergencia en los primeros días y luego se organizaron en espacios del colegio que en el momento estuvieran libres como eran salones, plazoletas, escaleras, teatro, patio …esta situación llevó al incremento del índice de deserción pues la incomodidad de ubicación, la falta de asignación de aulas y el desarrollo de actividades académicas en espacios no adecuados, bajó el nivel de motivación de los y las estudiantes por la permanencia en el colegio y elevó las cifras de abandono y deserción". (Ortega, 2010)[33].

Con la Resolución No. 161 del 24 de enero de 2008, se separa del Colegio Basilia la sede de ampliación Brasil López Quintana y se crea el *Colegio Germán Arciniegas*, llegando el primer rector de la institución el Licenciado Armando Ruiz Puerto, quien junto con su equipo de trabajo asumieron la responsabilidad de gestionar en el espacio que actualmente ocupa la Sede B del colegio Germán Arciniegas, ubicado en la calle 52 sur No. 97 B - 35, la adecuación de aulas prefabricadas para el desarrollo de las actividades académicas con un grupo de 1300 personas entre estudiantes, docentes, directivos docentes y administrativos, en medio de las difíciles condiciones generadas por no contar con dotación y una planta física propia y adecuada.

En la figura 7 se evidencia el registro fotográfico de las aulas prefabricadas en donde inicia su propia historia el colegio Germán Arciniegas, como una sede del colegio Brasil López Quintana (12 de mayo de 2007).

[33] COLEGIO GERMÁN ARCINIEGAS. Pacto de convivencia. [En línea]. Bogotá: Colegio Germán Arciniegas. 2018., 166 p. Disponible en: http://www.colegiogermanarciniegas.edu.co/institucional/PACTO-DE-CONVIVENCIA.pdf

Figura 7. Aulas prefabricadas.

Fuente registro fotográfico del colegio Germán Arciniegas.

En el año 2007, la Secretaría de Educación inicia la construcción del Colegio Germán Arciniegas ubicado en la carrera 88 I No. 54B – 44 sur, barrio Brasil I, de la localidad de Bosa; como se evidencia en el registro fotográfico de la Figura 8.

Figura 8. Proyecto de construcción del colegio Germán Arciniegas.

Fuente registro fotográfico del colegio Germán Arciniegas.

En el año 2010 es nombrada la rectora institucional Sorangela Miranda Beltrán, quien asumiendo el liderazgo de la Comunidad Educativa logra finalizar la construcción de la planta física del colegio y con el apoyo del Consejo Directivo y los padres de familia, logra la entrega de la infraestructura del colegio Germán Arciniegas y el 27 de Marzo de 2012, la totalidad de los estudiantes de Preescolar a Once se pasaron de las aulas prefabricadas a la actual llamada Sede A ubicada

en la carrera 88 I No. 54B – 44 sur, barrio Brasil I, de la localidad de Bosa; cambiando de manera significativa las condiciones en las cuales recibían el servicio educativo, al posesionarse de aulas especializadas, espacios recreo deportivos adecuados y agradables para el desarrollo de las tareas formativas. La institución fue diseñada con capacidad para 940 alumnos, 24 aulas, biblioteca, sala de proyecciones, aula múltiple, coliseo, aula de sistemas, laboratorios, comedor escolar, talleres de arte y ludoteca.

En el año 2013, la Dra. Sorangela Miranda, gestionó para la adquisición de los materiales de dotación para todo el colegio, accediendo a pupitres nuevos, salas de sistemas con las últimas tecnologías, biblioteca con más de 5000 mil ejemplares, laboratorios con los implementos necesarios para realizar las clases y excelentes espacios para el sano esparcimiento.

Se lidero la cultura del cuidado de la planta física y se encaminaron los esfuerzos a mantener las sedes con jardines y escenarios agradables para los estudiantes. Asimismo, se promovió la apertura de los procesos de media Integrada, la reformulación del Sistema Institucional de Evaluación (SIE), la puesta en marcha de los proyectos complementarios (fútbol, porras, artes) y se generó la participación del colegio en diversos eventos externos.

Teniendo en cuenta que la capacidad del colegio Germán Arciniegas fue diseñada para atender a 940 alumnos, con espacio para 24 aulas de clase, se proyectó con una la oferta educativa en jornada única con la proyección que se discrimina a continuación en la tabla 9.

Tabla 9. Oferta inicialmente proyectada para la I.E.D.

Grados	**Cantidad de**		
	Grupos	**Estudiantes por cada grupo**	**Total de estudiantes por grado**
Jardín	2	25	50
Transición	2	25	50
Primero	2	35	70
Segundo	2	35	70
Tercero	2	35	70
Cuarto	2	35	70
Quinto	2	35	70
Sexto	2	40	80
Séptimo	2	40	80
Octavo	2	40	80
Noveno	2	40	80
Décimo	2	40	80
Undécimo	2	40	80
Total	**26**	**465**	**930**

Fuente el autor

En razón a la situación de cobertura que presenta la localidad de Bosa siendo esta una localidad deficitaria, el colegio Germán Arciniegas presta sus servicios educativos en las jornadas mañana y tarde, adecuando la Sede provisional de Bosa el Porvenir (actual Sede B) para el año 2013 con resolución de aprobación SED No. 07-833 del 14 de mayo de 2014, abriendo más de mil cupos para los estudiantes de la localidad de Preescolar a grado Noveno, ampliando la planta de personal del colegio y contando con más recursos y dotación para el desarrollo de las actividades académicas.

En las tablas 10 y 11, se detalla la oferta educativa brindada por el Colegio Germán Arciniegas, desde el año 2008 hasta el 2017; en la tabla 10 se discrimina la cantidad de estudiantes por grado en cada año y en la tabla 11, se relacionan el total de estudiantes por año.

Tabla 10. Totales de la cobertura del año 2008 al 2017.

	Año									
Grado	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Jardín							97	100	91	97
Grado 0	162	168	165	154	169	306	159	151	147	148
Grado 1	228	161	164	164	180	456	329	162	244	235
Grado 2	223	245	162	159	179	338	442	341	152	276
Grado 3	212	238	248	173	181	308	329	445	354	153
Grado 4	197	245	246	244	183	314	292	334	447	337
Grado 5	195	229	232	230	254	321	306	299	335	442
Primaria Acelerada	50	55	52	55	55	103	89	46	25	47
Grado 6	238	196	184	169	182	406	291	330	302	328
Grado 7	237	230	170	160	170	318	368	296	326	295
Grado 8	84	241	243	159	166	253	285	357	290	304
Grado 9	85	92	243	221	157	168	221	273	323	272
Grado 10	75	82	86	219	205	177	153	197	233	252
Grado 11		75	70	68	150	176	154	142	143	187
Totales	1986	2257	2265	2175	2231	3644	3515	3473	3412	3373

Fuente el autor

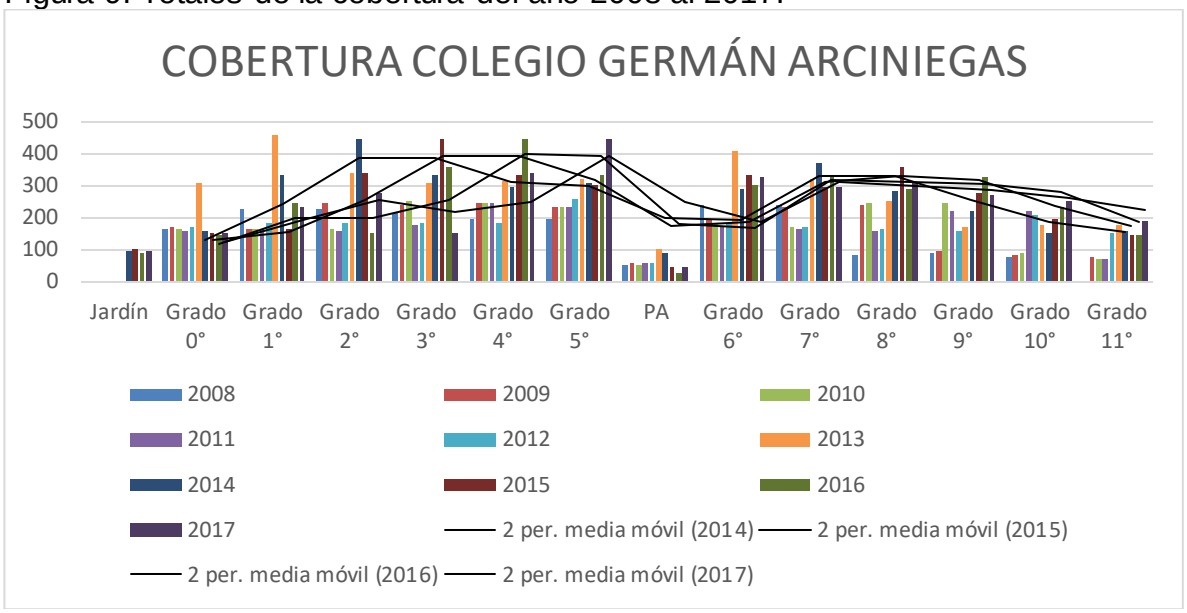
Tabla 11. Totales de la cobertura por año del 2008 al 2017.

Año	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Estudiantes	1986	2257	2265	2175	2231	3644	3515	3473	3412	3373

Fuente el autor

En la figura 9 se evidencia la prestación del servicio educativo, se discrimina por grados y por años la cobertura de la matrícula, como se relacionó en la tabla 10.

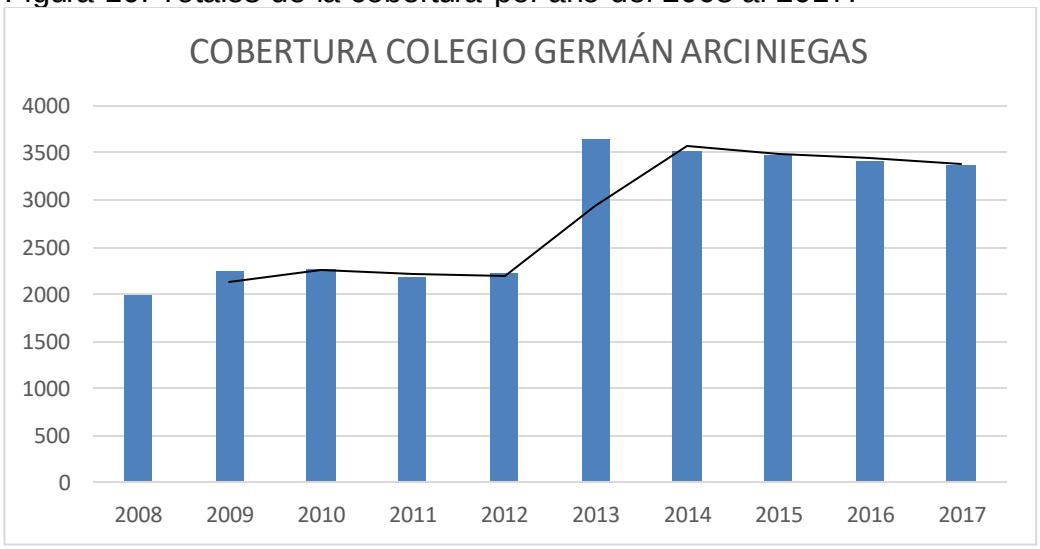
Figura 9. Totales de la cobertura del año 2008 al 2017.



Fuente el autor.

En la figura 10 se evidencia la prestación del servicio educativo con la cobertura de matrícula total por años, como se relacionó en la tabla 11.

Figura 10. Totales de la cobertura por año del 2008 al 2017.



Fuente el autor.

El Colegio Germán Arciniegas Institución Educativa Distrital, es de carácter oficial de Calendario A y para el año 2018 atiende una población total de 3200

estudiantes, en los niveles de educación preescolar, básica primaria, básica secundaria y media académica en las jornadas mañana y tarde; a la fecha ha proclamado 9 promociones de bachilleres, es decir 1116 bachilleres académicos, de los cuales 65 bachilleres de la jornada mañana y 511 de la jornada tarde como se describe en la tabla 12.

Tabla 12. Graduados desde el 2009 al 2017.

	Graduados	
Año	JM	JT
2009	28	42
2010	31	33
2011	32	32
2012	89	53
2013	90	79
2014	81	71
2015	72	66
2016	73	61
2017	109	74
Total	605	511

Fuente el autor.

Misión

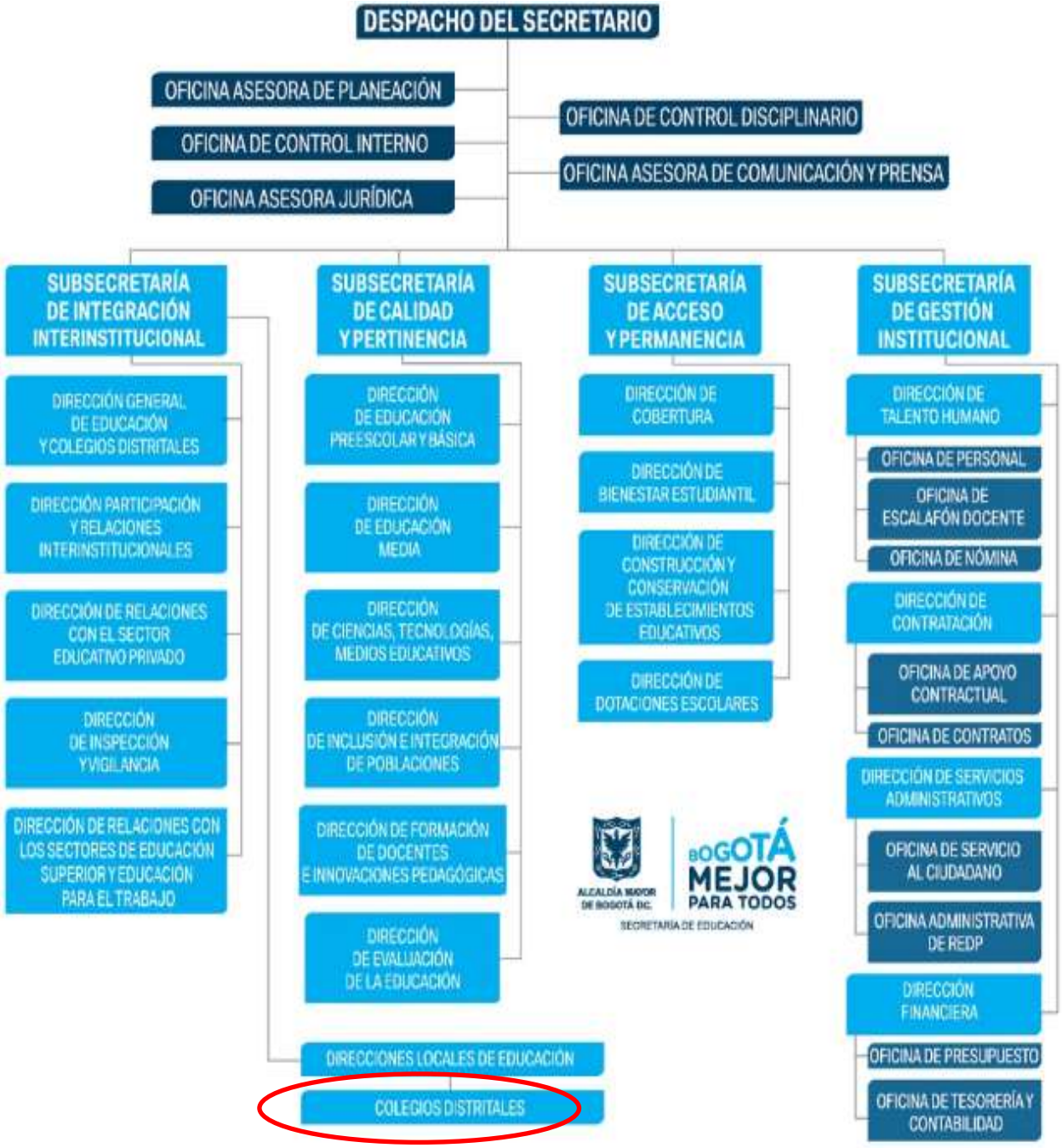
El Colegio Germán Arciniegas es una Comunidad Educativa formadora de líderes sociales, capaces de afrontar y resolver situaciones problemáticas de la cotidianidad al desarrollar su potencial humano, su autoestima, su creatividad, su capacidad participativa y su proyecto de vida. Esta comunidad se caracteriza por ser agente transformador del entorno familiar y social, promoviendo la educación de hombres y mujeres comprometidos con el cambio social en el marco de la integralidad, la mirada crítica reflexiva, el respeto por la diversidad y el aporte innovador en las dinámicas y exigencias de la sociedad de la información y el conocimiento[34].

Organigramas

A continuación, en la figura 11, se muestra el organigrama de la Secretaría de Educación del Distrito, donde se evidencia la ubicación del nivel institucional de la entidad, al cual pertenece el colegio Germán Arciniegas como Institución Educativa del Distrito.

[34] PACTO DE CONVIVENCIA. Óp. Cit., p. 24.

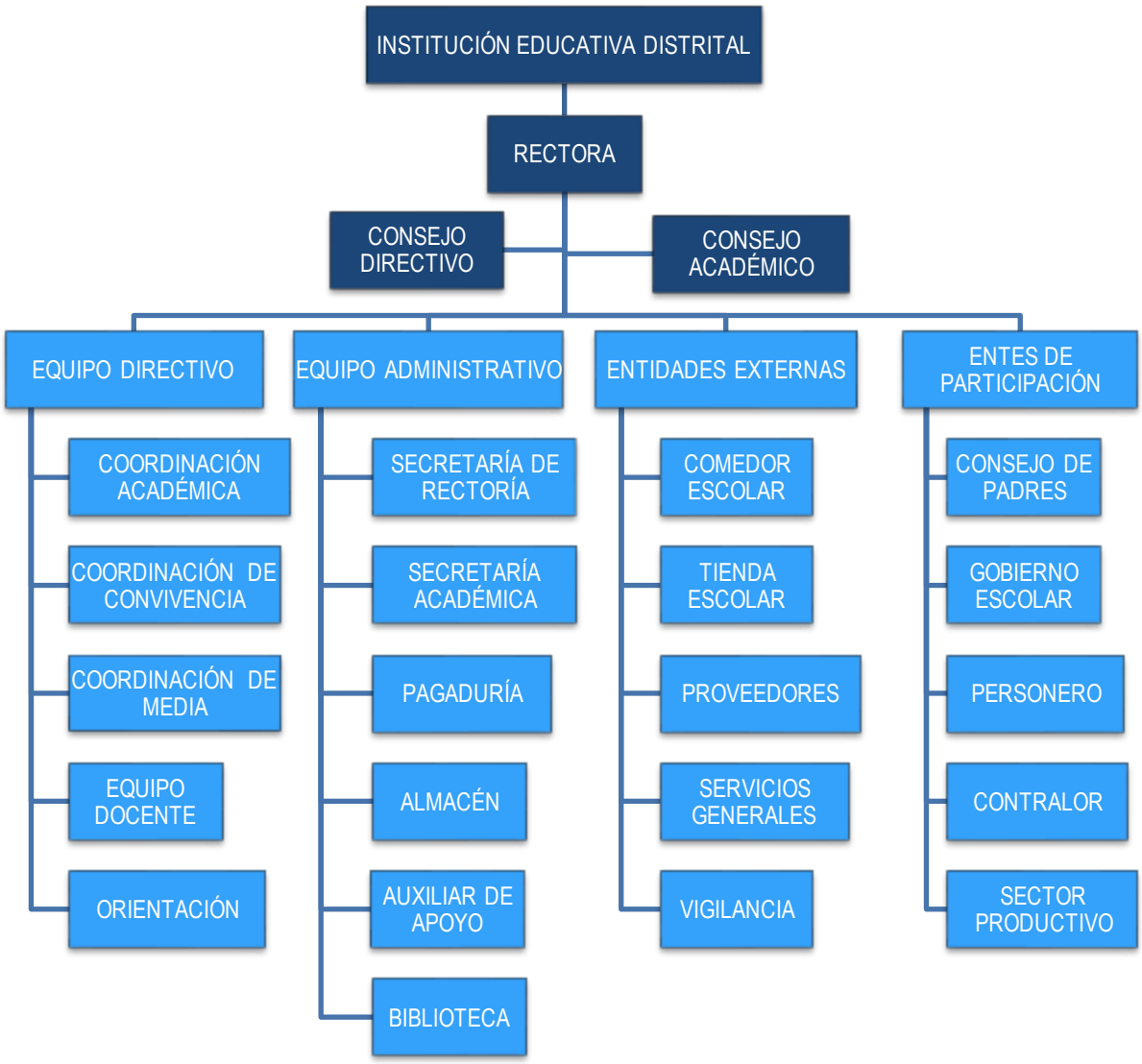
Figura 11. Organigrama de la Secretaría de Educación del Distrito.



Fuente http://www.educacionbogota.edu.co/es/nuestra-entidad/organigrama

En la figura 12 se muestra el organigrama del colegio Germán Arciniegas IED, dando continuidad al organigrama de la Secretaría de Educación del Distrito.

Figura 12. Organigrama del colegio Germán Arciniegas IED

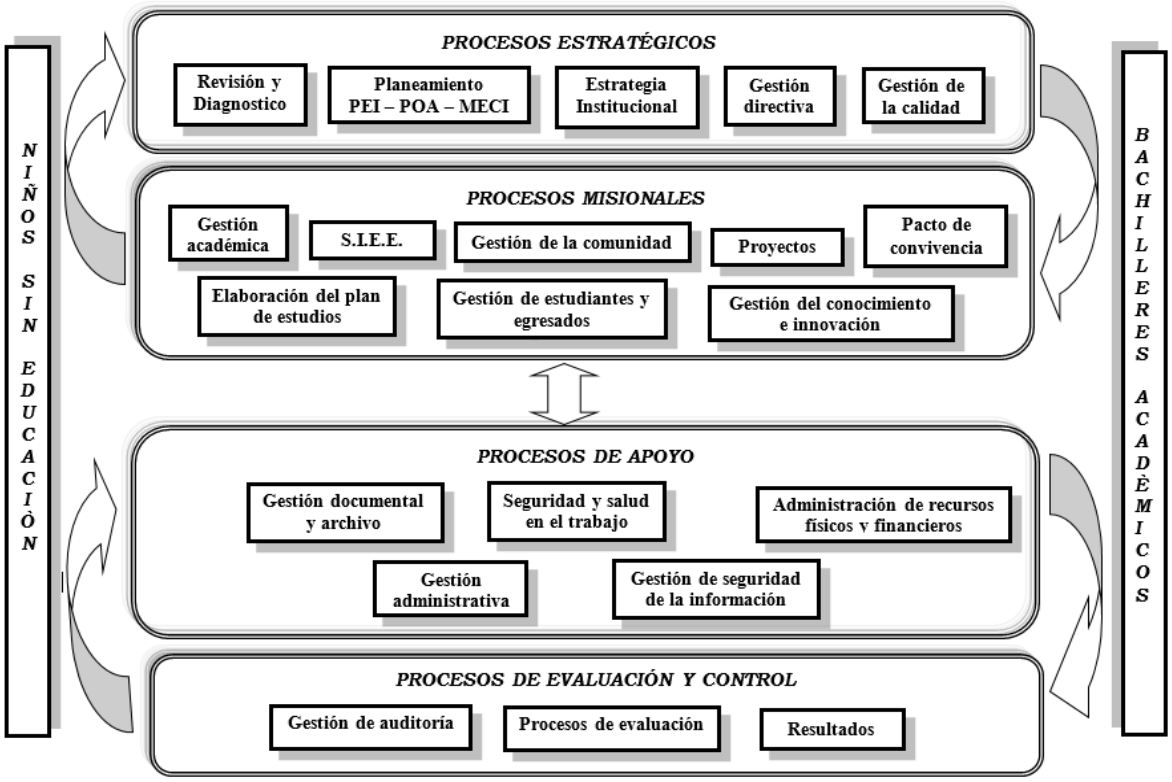


Fuente el autor.

Mapa de Procesos del colegio Germán Arciniegas IED.

Los procesos definidos en la institución educativa son los estratégicos, misionales, de apoyo, y de evaluación y control; los cuales reúnen todos los procesos de la IED como se evidencian en la figura 13, basados en el mapa de procesos diseñado por el ingeniero Giovanny Reyes.

Figura 13. Mapa de procesos colegio Germán Arciniegas.



Fuente el autor.

La Comunidad Educativa del colegio Germán Arciniegas IED, tiene como centro a sus estudiantes. Para la formación integral de los actores principales, unen los esfuerzos de los siguientes estamentos:

- Los directivos, encargados de dinamizar y motivar la acción educativa.
- El sector productivo, quienes, desde el ámbito económico, son gestores y promotores que afectan e inciden en el desarrollo integral y la vida de los y las estudiantes.
- La familia, como gestora y constructora de la formación de sus hijos.
- Los docentes quienes son los acompañantes y orientadores de los procesos de crecimiento de cada uno de los estudiantes.
- El personal administrativo que con su trabajo brinda ejemplo de servicio.
- Los orientadores quienes desde el ámbito profesional apoyan el mejoramiento continuo de la calidad educativa.
- El personal de servicios generales como formadores de la comunidad desde sus labores indispensables e imprescindibles para la institución y su testimonio de servicio.
- Los egresados debidamente organizados como canalizadores de las acciones educativas y gestores de los nuevos procesos en la realidad nacional[35].

[35] PACTO DE CONVIVENCIA. Óp. Cit., p. 21.

7.1.2. Comprensión de las necesidades y expectativas de las partes interesadas

Dentro de las necesidades de las partes interesadas se requiere dar a conocer las políticas y procedimientos del sistema de gestión de seguridad de la información al personal del colegio Germán Arciniegas, mediante capacitaciones que articulen, políticas públicas, contratación, CONPES, normatividad del SGSI, gestión de archivos, planes de mejora, aplicativos y herramientas tecnológicas.

Fortalecer la apropiación de la cultura digital, normatividad y políticas con respecto a las TIC, mediante el manejo de la gestión del riesgo que pueden afectar los activos de información, protegiendo la información y los datos de los estudiantes y sus familias.

Se requiere el apoyo y acompañamiento de la Secretaría de Educación en el proceso de implementación del SGSI en el colegio Germán Arciniegas, mediante la asignación de recursos físicos, financieros y de talento humano, capacitaciones, aplicativos y herramientas que permitan la protección de los activos de información.

Las expectativas de las partes interesadas frente al sistema de gestión de seguridad de la información, es lograr sensibilización al personal de la entidad el cumplimiento de las políticas de seguridad, evitar la pérdida de información o daños en sistemas informáticos mediante la implementación de la gestión del riesgo del SGSI, garantizar la confidencialidad, seguridad, integridad y acceso a la información incrementando el uso de las tecnologías de la información.

El diseño del sistema de gestión de seguridad de la información para el colegio Germán Arciniegas, tendrá la estructura para su implementación, seguimiento y mejora, se espera que mediante el apoyo de la Secretaría de Educación este diseño sea implementado.

7.1.3. Determinación del alcance del sistema de gestión de la seguridad de la información

El alcance del sistema de gestión de seguridad de la información para el colegio Germán Arciniegas abarca todos los activos de la información y manejo de datos involucrados en la gestión de archivo de los procesos institucionales, estos procesos son estratégicos, misionales, de apoyo de evaluación y control.

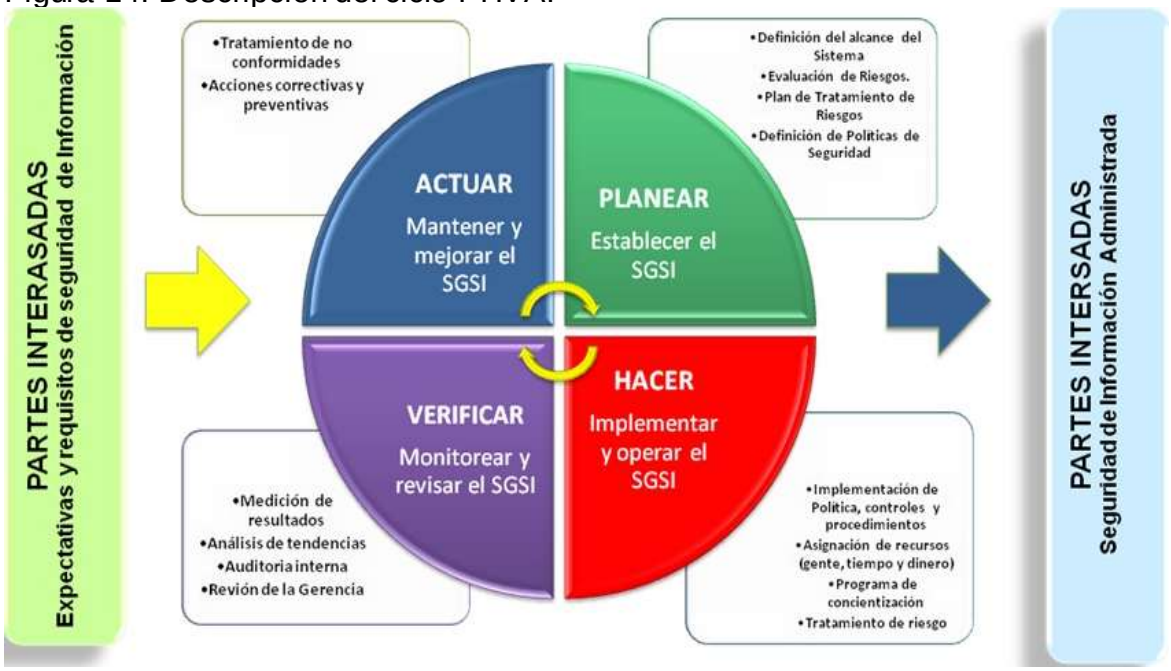
La información contenida en cada uno de los procesos institucionales se encuentra en documentos físicos o formato papel, en diferentes medios de

almacenamiento, bases de datos, correos electrónicos y los sistemas de información los cuales impactan directamente la consecución de objetivos misionales.

7.1.4. Sistema de gestión de la seguridad de la información

En la implementación del sistema de gestión de seguridad de la información se utiliza el ciclo PDCA por sus siglas en inglés o PHVA por sus siglas en español de planear, hacer, verificar y actuar como se describe en la figura 14. En estas fases se permite medir el estado del SGSI con el fin de realizar la mejora continua, para el SGSI del colegio Germán Arciniegas, se desarrollarán las siguientes fases:

Figura 14. Descripción del ciclo PHVA.



Fuente http://toddleoutsourcing.es/wp-content/uploads/2014/04/sgsi_pdca.jpg

El funcionamiento del SGSI es a través de la descripción detallada de cada una de las fases que lo comprenden. En la fase del diagnóstico se conoce el estado actual de la institución mediante el levantamiento de la información, seguidamente se tienen las fases de planeación, de implementación, evaluación del desempeño y de mejora continua. En la figura 15 se describe los procesos a realizar en cada una de las fases.

Figura 15. Procesos de las fases que comprenden el SGSI.

Fuente el autor.

7.1.5. Integración del modelo de seguridad y privacidad de la información - MSPI, con el Sistema de Gestión documental.

La Gestión Documental del colegio Germán Arciniegas se enfoca en las directrices dadas por la Secretaría de Educación del Distrito, la cual se encuentra enmarcada y articulada con las disposiciones de las siguientes normas:

- Ley 594 de 2000. Ley General de Archivos.
- Ley 1581 de 2012
- Ley 1712 de 2014
- Decreto 1080 de 2015
- Decreto 2578 de 2012
- Acuerdos reglamentarios del Archivo General de la Nación a partir del año 2000

La Secretaría de Educación del Distrito adopta el programa de Gestión Documental mediante Resolución 599 de 2014[36], el Comité Interno de Archivo es

[36] SECRETARÍA DE EDUCACIÓN DEL DISTRITO. Resolución 599. (28, marzo, 2014). Por medio de la cual se conforma el Comité Interno de Archivo de la Secretaria de Educación del Distrito, se reglamenta su funcionamiento y se deroga la Resolución 856 del 25 de abril de 2012. Bogotá D.C. 2014. [En línea]. Disponible http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=60457

la máxima instancia asesora de la gestión documental de la entidad, la Subsecretaría de Gestión Institucional es la oficina que a nivel directivo tiene a su cargo la función archivística y la representación institucional ante el Archivo de Bogotá. La instancia coordinadora, ejecutora y responsable del seguimiento a la implementación del Programa de Gestión Documental en la Secretaría de Educación del Distrito es la Dirección de Servicios Administrativos, la cual tiene como responsabilidad el desarrollo institucional de la gestión documental.

La Secretaría de Educación Distrital, actualmente se encuentra trabajando en el desarrollo de la Tabla de Retención Documental para el nivel institucional, sin embargo cada oficina de la institución educativa productora de documentos cuenta con su archivo de gestión el cual ha organizado y clasificado acorde con las directrices dadas en las capacitaciones en gestión documental, dirigido a los funcionarios de los diferentes niveles de la SED.

La Gestión Documental de la Secretaría de Educación del Distrito se encuentra normalizada a través de los siguientes documentos:

- Política institucional de gestión documental
- Programa de gestión documental - PGD
- Reglamento interno de gestión documental
- Plan institucional de archivos de la entidad – PINAR

Las actividades planteadas en el programa de gestión documental desarrollan las siguientes líneas estratégicas de la Política Institucional de Gestión Documental:

- Política, responsabilidades y procesos.
- Gestión de documentos físicos y electrónicos.
- Fortalecimiento en talento humano.
- Fortalecimiento de la formación en gestión documental y gestión del cambio.
- Adopción y actualización permanente de la regulación de gestión documental.
- Modernización e Incorporación de tecnologías de la información y la comunicación[37].

El PGD de la Secretaría de Educación del Distrito define las directrices y actividades para cada una de las etapas del ciclo de vida de los documentos y se enmarca dentro del concepto de archivo total, que de acuerdo con el Decreto 1080 de 2015[38], comprende los procesos plasmados en la figura 16.

[37] GUZMÁN LUCERO, Álvaro Fernando. Programa de gestión documental Secretaría de Educación del Distrito. [En línea]. Bogotá: Secretaría de Educación del Distrito. 2017., 41 p. Disponible en: https://www.educacionbogota.edu.co/archivos/Nuestra_Entidad/Gestion/Gestion%20Documental/2018/Programa_gestion_documental_2017.pdf

[38] EL PRESIDENTE DE LA REPÚBLICA. Decreto 1080. (26, mayo, 2015). Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura. Bogotá D.C. La Ministra de Cultura. 2015. [en línea]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=62515

Figura 16. Etapas del ciclo de vida de los documentos.

Fuente programa de gestión documental 2017.

Teniendo en cuenta el ciclo vital de los documentos, la Secretaría de Educación del Distrito ha implementado las siguientes fases de archivo:

- ⇨ Archivo de gestión: comprende el archivo no superior a dos años inmediatamente anteriores de su producción y continúa siendo utilizado y consultado.
- ⇨ Archivo central: comprende el archivo entre 2 y 20 años anteriores de su producción y su consulta no es muy frecuente.
- ⇨ Archivo histórico: como su nombre lo indica es de carácter histórico y supera los 20 años de su producción.

7.2. LIDERAZGO

7.2.1. Liderazgo y compromiso

La Política de la Seguridad de la Información de la Secretaría de Educación del Distrito, aplica a todos los servidores públicos, contratistas, terceros, aprendices, practicantes, usuarios y en general a todas las personas que de manera directa o indirecta hagan uso de la información ofrecida por la entidad en el nivel central, local e institucional. El uso no adecuado e incumplimiento de política de seguridad de la información de la SED, da lugar a la aplicación de las medidas administrativas, disciplinarias o legales.

El colegio Germán Arciniegas pertenece al nivel institucional de la SED, por lo tanto la Política de Seguridad de la Información establecida por la Secretaría de

Educación en la Resolución 1944 del 27 de octubre de 2016, rige para la institución educativa y todos sus funcionarios teniendo en cuenta que los funcionario públicos deben cumplir y hacer que se cumplan, las leyes, los decretos, las ordenanzas, los acuerdos distritales y municipales, los estatutos de la entidad, los reglamentos y los manuales de funciones[39]. En la institución educativa el liderazgo del cumplimiento de la política está a cargo de la rectora de la institución Dra. Sorangela Miranda Beltrán.

7.2.2. Política

Política de Seguridad de la Información de la SED

La Secretaría de Educación del Distrito, adopta la Política de seguridad de la información para la entidad en sus niveles central, local e institucional; mediante la Resolución N°. 1944 del 27 de octubre del 2016. La Secretaría de Educación del Distrito, implementará y divulgará la política y sus lineamientos, teniendo en cuenta los siguientes aspectos:

- Organizativos de la seguridad de la información
- Seguridad de los recursos humanos
- Gestión de activos
- Control de accesos
- Cifrado
- Seguridad física y ambiental
- Seguridad operativa
- Seguridad en las telecomunicaciones
- Adquisición, desarrollo y mantenimiento de los sistemas de información
- Relaciones con proveedores
- Gestión de incidentes en la seguridad de la información
- Gestión de la continuidad del negocio
- Cumplimiento

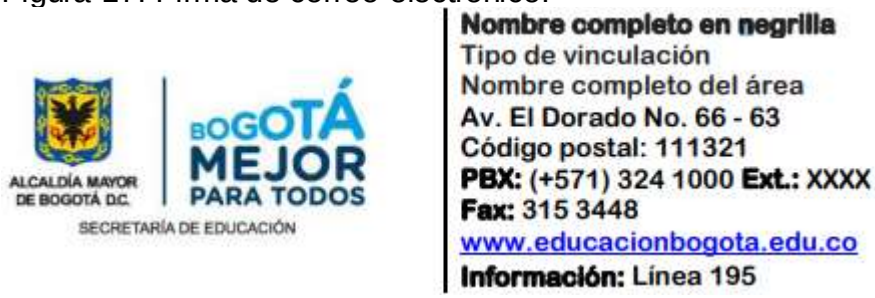
El colegio Germán Arciniegas Institución Educativa Distrital, debe adoptar la política de seguridad de la información de la Secretaría de Educación del Distrito, establecida mediante Resolución N°. 1944 del 27 de octubre del 2016. Estas políticas se encuentran publicadas en la página web de la SED, en la siguiente URL: http://www.educacionbogota.edu.co/es/temas-estrategicos/transparencia-y-gestion-publica/politica-de-seguridad-de-la-informacion, donde se presentan las políticas para el uso y manejo del correo electrónico, las política de privacidad y condiciones de uso de portales WEB y las política de Tratamiento de datos personales.

[39] CONGRESO DE COLOMBIA. Ley 734. (05, 02, 2002). por la cual se expide el código único disciplinario. 147 p.

En las políticas para uso y manejo del correo electrónico se presentan los lineamientos para los usuarios del correo electrónico, indicaciones de las acciones que no son permitidas, directrices para el uso de correos masivos o grupos de distribución y las características para la firma del correo electrónico, la cual se muestra en la figura 17.

Firma del correo

Figura 17. Firma de correo electrónico.



Fuente:
www.educacionbogota.edu.co/archivos/SECRETARIA_EDUCACION/Transparencia%20y%20acceso%20a%20informacion/2017/Politica_uso_manejo_correo_electronico.pdf

Las políticas de privacidad y condiciones de uso de portales WEB contienen la producción de contenidos, los lineamientos de los derechos de propiedad intelectual – Copyright, información de servicios en línea para la ciudadanía, las condiciones de uso para los portales web. Adicionalmente se presentan algunos vínculos que tienen como propósito informar al usuario sobre la existencia de otras fuentes susceptibles de ampliar los contenidos o que guardan relación con aquellos. Estos vínculos son relacionados en la tabla 13.

Tabla 13. Links de los portales web de consultas.

Links de consultas	Portales web
http://www.educacionbogota.edu.co/es/nuestra-entidad/transparencia-informacion-publica	Transparencia y acceso a la información pública de la SED.
http://www.redacademica.edu.co/	Red académica de la SED.
http://repositoriosed.educacionbogota.edu.co/jspui/	Repositorio institucional de la Secretaría de Educación Distrital.
http://www.educacionbogota.edu.co/es/sitios-de-interes/nuestros-sitios/agencia-de-medios	Agencia de medios de la Secretaría de Educación Distrital.

Fuente el autor.

Por otra parte en las políticas de privacidad y condiciones de uso de portales WEB se presentan las características para la aceptación de términos, privacidad y responsabilidad, modificaciones a las condiciones de uso, la duración de la prestación del servicio de los portales web de la SED y la seguridad de la información y con las medidas de seguridad.

En la política de tratamiento de datos personales se determina el tratamiento de datos sensibles, se establece los casos para autorización del titular, los casos en que no se requiere la autorización del titular, los criterios para suministrar información personal, las condiciones que las personas deben cumplir para el tratamiento de sus datos, los casos en que no requiere autorización del titular y las características de las personas a quienes se les puede suministrar la información personal.

La política del tratamiento de datos personales de niños y adolescentes, busca fundamentalmente darle el uso correspondiente a esta información, respondiendo a su interés superior, de acuerdo con las disposiciones de la Ley 1581 de 2012, artículo 7.

Se relacionan los deberes de la Secretaría de Educación en relación con el tratamiento de los datos personales como responsable del tratamiento de datos personales, se mencionan los criterios para las autorizaciones y consentimientos, el alcance y contenido del aviso de privacidad, prerrogativas y demás derechos de los titulares de la información, las garantías del derecho de acceso a la información y criterios de consulta así como los de los reclamos, proceso para la eliminación, rectificación y actualización de datos

7.2.3. Roles, responsabilidades y autoridades en la organización

Teniendo en cuenta el mapa de procesos y el organigrama institucional, en la tabla 14, se describen los procesos realizados en el colegio Germán Arciniegas con las actividades generales realizadas en cada proceso y sus respectivos responsables, la información que se genera en estos, debe ser tratada por el personal a cargo de la actividad.

Tabla 14. Procesos, actividades y responsables.

Proceso	Actividades de los procesos	Responsables
Procesos estratégicos	Estrategia institucional	Rectoría y equipo directivo
	Gestión de la calidad	Todo el personal de la IED
	Gestión directiva	Rectoría y equipo directivo
	Planteamiento del PEI-POA-MECI	Rectoría y equipo directivo
	Revisión y diagnóstico	Rectoría y equipo directivo
Procesos misionales	Elaboración del plan de estudios	Rectoría, equipos directivo y docente
	Gestión académica	Rectoría, equipos directivo y

Proceso	Actividades de los procesos	Responsables
		docente
	Gestión de estudiantes y egresados	Rectoría, equipos directivo y docente
	Gestión de la comunidad	Rectoría, equipos directivo y docente
	Gestión del conocimiento e innovación	Rectoría, equipos directivo y docente
	Pacto de convivencia	Rectoría, equipos directivo, docente y de orientadores
	Proyectos	Rectoría, equipos directivo y docente
	S.I.E.E.	Rectoría, equipos directivo y docente
Procesos de apoyo	Administración de recursos físicos y financieros	Consejo Directivo.
	Gestión Administrativa	Rectoría y equipo administrativo
	Gestión de Seguridad de la Información	Todo el personal de la IED
	Gestión documental y de archivo	Todo el personal de la IED
Procesos de evaluación y control	Gestión de auditoría	Secretaría académica
	Procesos de evaluación	Rectoría
	Resultados	Rectoría

Fuente el autor.

Con respecto al sistema de gestión de seguridad de la información en el colegio Germán Arciniegas como institución educativa de la Secretaría de Educación, se tienen que los dominios y las responsabilidades del SGSI definidos por la SED, son los relacionados en la tabla 15.

Tabla 15. Dominios del SGSI.

DOMINIO	RESPONSABILIDADES	RESPONSABLE
SERVICIOS TECNOLÓGICOS	Liderar la gestión de riesgos de seguridad sobre la gestión de TI y de información de la institución. Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de gestión de TI e información. Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad. Supervisar la respuesta a incidentes, así como la	Oficina de REDP de la SED

DOMINIO	RESPONSABILIDADES	RESPONSABLE
	investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias. Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio. Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información.	
ESTRATEGIA TI	Definir la estrategia informática que permita lograr los objetivos y minimizar de los riesgos de la institución. Es el encargado de guiar la prestación del servicio y la adquisición de bienes y servicios relacionados y requeridos para garantizar la seguridad de la información.	Oficina de REDP de la SED
GOBIERNO TI	Seguir y controlar la estrategia de TI, que permita el logro de los objetivos y la minimización de los riesgos del componente de TI. Encargado monitorear y gestionar la prestación del servicio y la adquisición de bienes y/o servicios relacionados y requeridos para garantizar la seguridad de información.	Oficina de REDP de la SED
SISTEMAS DE INFORMACIÓN	Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro de la entidad. Apoyar la implementación segura de los sistemas de información, de acuerdo con el modelo de seguridad y privacidad de la información del estado colombiano. Desarrollar pruebas periódicas de vulnerabilidad sobre los diferentes sistemas de información para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información. Liderar el proceso de gestión de incidentes de seguridad así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados. Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio.	Oficina de REDP de la SED

DOMINIO	RESPONSABILIDADES	RESPONSABLE
DE INFORMACIÓN	Supervisar que se garantice la confidencialidad, integridad y disponibilidad de la información a través de los distintos componentes de información implementados. Verificar el cumplimiento de las obligaciones legales y regulatorias del estado relacionadas con la seguridad de la información.	Oficina de REDP de la SED
USO Y APROPIACIÓN	Desarrollar el plan de formación y sensibilización de la entidad incorporando el componente de seguridad de la información en diferentes niveles. Supervisar los resultados del plan de formación y sensibilización establecido para la entidad, con el fin de identificar oportunidades de mejora. Participar en la elaboración de los planes de gestión de cambio, garantizando la inclusión del componente de seguridad de la información en la implementación de los proyectos de TI.	Oficina de REDP de la SED

Fuente Guía No. 4 de seguridad y privacidad de la información.

El sistema de gestión de seguridad de la información en el colegio Germán Arciniegas estará liderado por la rectora Sorangela Miranda Beltrán y contará con el apoyo de las administrativas Sandra Patricia Munévar Flechas secretaria de rectoría y Carolina Figueroa Cubillos secretaria académica.

7.3. PLANIFICACIÓN

7.3.1. Acciones para tratar riesgos y oportunidades

Mediante la aplicación de una encuesta web al personal docente, administrativo y directivo de la institución educativa, se levanta el inventario inicial de activos de la información. Las preguntas del formulario aplicado son las que se evidencian en la figura 18.

Figura 18. Formulario web.

Fuente el autor.

Las respuestas del formulario web se registraban en una tabla en formato Excel, donde se obtuvieron los registros de las respuestas suministradas por los funcionarios del colegio, como se evidencia en la figura 19.

Figura 19. Respuestas formulario web.

Fuente el autor.

Dentro del inventario de activos, se encontraron los siguientes tipos de activos de acuerdo con la clasificación de la metodología Margerit, como se evidencia en la tabla 16.

Tabla 16. Tipos de activos

Categoría	Activo	Cantidad	Descripción de activos
[D]	Datos / Información	N.A.	Actas
		N.A.	Bases de datos
		N.A.	Circulares
		N.A.	Comunicados
		N.A.	Correspondencia
		N.A.	Documentos
		N.A.	Formatos
		N.A.	Formularios
		N.A.	Informes
		N.A.	Libros
		N.A.	Listados
		N.A.	Oficios
		N.A.	Registros
		N.A.	Resoluciones
[K]	Claves criptográficas	1	Equipo de cómputo de Rectoría
		6	Equipos de cómputo de funcionarios administrativos
		4	Equipos de cómputo de orientadores
		3	Equipos de cómputo de coordinadores
		1	Equipo de cómputo de bibliotecaria

Categoría	Activo	Cantidad	Descripción de activos
[S]	Servicios	N.A.	Agendamiento de citas para atención personalizada
		N.A.	Consulta de circulares
		N.A.	Consulta de contenidos programáticos
		N.A.	Requisitos de matrícula.
		N.A.	Solicitudes de constancias de asistencia de estudiantes activos – Web
		N.A.	Solicitudes de constancias y certificados de estudiantes activos - Web
[SW]	Software / Aplicaciones informáticas	1	Aplicativo de verificación de asistencia
		1	Ficha de referenciación y autorización de contacto línea psicoactiva.
		1	Página web institucional
		1	Sistema Biométrico del Colegio Germán Arciniegas
		1	Sistema de alertas de la Secretaria Educación Distrital
		1	Sistema de integrado de gestión de la correspondencia - SIGA
		1	Sistema de matrículas - SIMAT
[HW]	Equipamiento informático (hardware)	28	Equipo de escritorio marca DELL
		50	Equipos de escritorio marca HP
		1	Equipos de escritorio marca lenovo
		30	Equipos portátiles marca HP
		10	Equipos portátiles marca lenovo
		55	Tabletas del programa computadores para educar
		114	Tabletas ZTE
[COM]	Redes de comunicaciones	20	Access Point AP 93
		27	Puntos de red de datos
		29	Puntos eléctricos regulados
		1	Regulador
		1	Rack de pared de 5 RMS
		N.A.	Red LAN
		N.A.	Red telefónica
		N.A.	Red Wifi
		1	Router CISCO 2900
		1	Switch de 48 puertos
		1	Switch de 24 puertos
		1	Switch de 8 puertos
		1	Tablero eléctrico
			Tubería EMT
[Media]	Soportes de información	30	CD
		1	Disco duro externo

Categoría	Activo	Cantidad	Descripción de activos
		10	DVD
		10	USB
[AUX]	Equipamiento auxiliar	N.A.	Cableado UTP categoría 6
		N.A.	Canaleta de calibre 22 12X5
		N.A.	Fibra óptica OM3
[L]	Instalaciones	N.A.	Planta física de la sede A del colegio Germán Arciniegas IED
[P]	Personal	6	Administrativos
		1	Bibliotecario
		3	Coordinadores
		75	Docentes
		4	Orientadores
		1	Rectora

Fuente el autor.

Una vez identificados los activos de la información que se maneja en el colegio Germán Arciniegas y el alcance definido, se clasifican según los diferentes tipos de activos y se diligencia la matriz de activos de la información que se encuentra en formato Excel. El formato de esta matriz es suministrado por la Secretaría de Educación del Distrito y en esta se determina la ubicación del activo, su responsable, el nivel de criticidad de acuerdo con sus niveles de confidencialidad, integridad y disponibilidad.

La valoración y clasificación del activo se realiza teniendo en cuenta el sistema de clasificación de la información que se establece en la gestión de activos de los estándares 27001:2013, ISO 27002, e ISO 27005, el cual tiene como objetivo asegurar que la información recibe los niveles de protección adecuados, ya que con base en su valor y de acuerdo a otras características particulares, requiere un tipo de manejo especial de acuerdo con los criterios relacionados en la tabla 17.

Tabla 17. Clasificación de los niveles de protección.

CONFIDENCIALIDAD	ALTA	Información disponible sólo para procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo.
	MEDIA	Esta información es propia de la entidad y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
	BAJA	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a las actividades y procesos de la entidad.
	NO CLASIFICADA	Activos de información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PUBLICA RESERVADA.

INTEGRIDAD	ALTA	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo para la entidad.
	MEDIA	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo, retrasar sus funciones, o generar pérdida moderada a en la entidad.
	BAJA	La pérdida de exactitud y completitud de la información, tiene un impacto no significativo para la entidad.
	NO CLASIFICADA	Los activos de información no han sido clasificados, deben ser tratados como activos de información de integridad ALTA.
DISPONIBILIDAD	ALTA	La no disponibilidad de la información puede conllevar un impacto negativo muy alto o generar pérdidas severas.
	MEDIA	La no disponibilidad de la información puede conllevar un impacto negativo, retrasar funciones o generar pérdidas moderadas para la entidad.
	BAJA	La no disponibilidad de la información puede afectar la operación normal de la entidad pero no genera impactos negativos o pérdidas graves.
	NO CLASIFICADA	Los activos de la información que no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA.

Fuente el autor.

En la matriz de activos de la información se evidencia que los activos que forman parte del alcance definido para el SGSI del colegio Germán Arciniegas, son los que conforman el porcentaje más alto del inventario, como se evidencia en la tabla 18.

Tabla 18. Inventario de los activos de la información.

Activos	Tipo	Cantidad
Datos / Información	[D]	344
Hardware	[HW]	97
Software	[SW]	7
Claves criptográficas	[K]	15
Servicios	[S]	5
Redes de comunicaciones	[COM]	83
Soportes de información	[Media]	40
Equipamiento auxiliar	[AUX]	3
Instalaciones	[L]	1
Personal	[P]	90
Total		685

Fuente el autor.

En la figura 20, se puede evidenciar de manera gráfica los valores de los activos de la información y especialmente aquellos que forman parte de la gestión documental del colegio Germán Arciniegas.

Figura 20. Inventario de activos de la información.

Fuente el autor

7.3.2. Identificación, valoración y tratamiento de riesgos.

Para la valoración de los riesgos, se tienen en cuenta la metodología MARGERIT, de donde se definen las escalas cualitativas relacionadas en la tabla 19.

Tabla 19. Escalas cualitativas

Impacto	Probabilidad	Riesgo
MB: Insignificante	MB: Raro	MB: Muy bajo
B: Menor	B: Improbable	B: Bajo
M: Moderado	M: Posible	M: Medio
A: Mayor	A: Probable	A: Alto
MA: Catastrófico	MA: Casi seguro	MA: Muy alto

Fuente el autor.

El análisis de riesgo, se realiza combinando el impacto con la probabilidad de ocurrencia, donde se tiene la valoración relacionada en la tabla 20, con el respectivo mapa de calor.

Tabla 20. Análisis del riesgo

		Probabilidad				
	Riesgo	MB	B	M	A	MA
Impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente el autor.

Adicionalmente se define en el mapa de riesgos, la medida de respuesta al análisis de riesgos con la valoración relacionada en la tabla 21.

Tabla 21. Medida de respuesta

Evaluación del riesgo	Medida de Respuesta
MB: Muy bajo	Asumir el Riesgo
B: Bajo	Asumir el Riesgo
M: Moderado	Asumir el riesgo, reducir el riesgo
A: Alto	Asumir el riesgo, reducir el riesgo, evitar, compartir o transferir
MA: Extremo	Reducir el riesgo, evitar, compartir o trasferir

Fuente el autor.

Las medidas de respuestas a la evaluación del riesgo, tienen las siguientes acciones a realizar:

- El asumir el riesgo implica enfrentar la situación adversa, sin modificar el plan de gestión de riesgos.

- Reducir el riesgo hace referencia a la disminución de la probabilidad de ocurrencia y/o de la consecuencia.

- Evitar el riesgo busca la eliminación de las amenazas y vulnerabilidades que representan el evento negativo.

- Compartir o trasferir el riesgo hace referencia al traspaso del impacto negativo o amenaza a terceros dándole la responsabilidad de su administración.

En el mapa de riesgos se identifican las respectivas causas y consecuencias de los riesgos, la valoración de estos de acuerdo con la probabilidad y el impacto de ocurrencia y la medida de respuesta, como se evidencia en la tabla 22.

Tabla 22. Matriz de análisis de riesgos

2. IDENTIFICACIÓN DEL RIESGO					3. ANÁLISIS DEL RIESGO			
No.	Causas	Riesgo	Consecuencias	Tipo de Riesgo	Probabilidad	Impacto	Evaluación	Medida de Respuesta
1	Sobrecarga eléctrica Corto circuito	Eléctrico	Incendio	Riesgo de Tecnología	Improbable	Mayor	Alta	Asumir el riesgo, evitar, compartir o transferir
2	Humedad Polvo Contaminación	Ambiental	Pérdida o daño de la información	Riesgo de Gestión Documental	Posible	Moderado	Alta	Asumir el riesgo, evitar, compartir o transferir
3	Plagas Epidemias Roedores	Biológico	Pérdida o daño de la información	Riesgo de Gestión Documental	Posible	Moderado	Alta	Asumir el riesgo, evitar, compartir o transferir
4	Inundaciones Sismo Rayos	Naturales o físicos	Pérdida o daño de la información y de equipos.	Riesgo de Tecnología	Raro	Mayor	Alta	Asumir el riesgo, evitar, compartir o transferir
5	Desconocimiento de las políticas de seguridad Malos hábitos en el manejo de la información Carencia de un plan de capacitación	Humano	Pérdida o daño en la información	Riesgo de Gestión Documental	Posible	Mayor	Extrema	Asumir el riesgo, evitar, compartir o transferir
6	Carece de un plan de mantenimiento Inventario de los equipos Desconocimiento de los protocolos en el manejo de equipos.	Hardware	Daño, pérdida o robo en los equipos y pérdida o robo de la información	Riesgo de Tecnología	Improbable	Mayor	Alta	Asumir el riesgo, evitar, compartir o transferir
7	Contraseñas débiles Antivirus desactualizado Descarga de archivos o programas de dudosa procedencia	Software	Daños por virus informático, ataques por intrusos, daño, robo, pérdida o alteración de programas, bases de datos e información institucional.	Riesgo de Tecnología	Posible	Mayor	Extrema	Asumir el riesgo, evitar, compartir o transferir

Fuente el autor.

Posteriormente, en la valoración del riesgo se identifican los controles existentes, el tipo de control es preventivo dado que en la institución no se han presentado eventos que generen acciones correctivas; adicionalmente se determinan las acciones de mitigación de los riesgos, como muestra la tabla 23.

Tabla 23. Matriz de la valoración del riesgo

4. VALORACIÓN DEL RIESGO									
Controles existentes	Tipo de control	Criterios de valoración de control	Puntaje	Puntaje Final	Acciones de Mitigación				
					Acción de Mitigación	Fecha Inicio	Fecha Fin	Responsable	Indicador
Energía regulada	Preventivo	¿El control es automático?	15	55	Revisión de las toma corrientes eléctricas	31/07/2018	15/12/2018	Equipo de trabajo	
		¿El control es manual?	10						
		En el tiempo definido que lleva la herramienta ha demostrado ser efectiva	30						
Terminales a tierra	Preventivo	¿El control es automático?	15	55	Revisión de las toma corrientes eléctricas	31/07/2018	15/12/2018	Equipo de trabajo	
		¿El control es manual?	10						
		En el tiempo definido que lleva la herramienta ha demostrado ser efectiva	30						
Temperatura ambiente	Preventivo	No existe control	0	0	Control de temperatura y limpieza	31/07/2018	15/12/2018	Equipo de trabajo	
Limpieza	Preventivo	¿El control es manual?	10	55	Digitalización de la información	31/07/2018	15/12/2018	Equipo de trabajo	
		La frecuencia de la ejecución del control y seguimiento es adecuada	15						
		En el tiempo definido que lleva la herramienta ha demostrado ser efectiva	30						
Separación de residuos	Preventivo	¿El control es manual?	10	55	Gestión del PIGA	31/07/2018	15/12/2018	Equipo de trabajo	
		La frecuencia de la ejecución del control y seguimiento es adecuada	15						

4. VALORACIÓN DEL RIESGO									
Controles existentes	Tipo de control	Criterios de valoración de control	Puntaje	Puntaje Final	Acciones de Mitigación				
					Acción de Mitigación	Fecha Inicio	Fecha Fin	Responsable	Indicador
		En el tiempo definido que lleva la herramienta ha demostrado ser efectiva	30						
Fumigación	Preventivo	¿El control es manual?	10	25	Fumigación periódica	31/07/2018	15/12/2018	Equipo de trabajo	
		La frecuencia de la ejecución del control y seguimiento es adecuada	15						
Fumigación	Preventivo	¿El control es manual?	10	25	Fumigación periódica	31/07/2018	15/12/2018	Equipo de trabajo	
		La frecuencia de la ejecución del control y seguimiento es adecuada	15						
Fumigación	Preventivo	¿El control es manual?	10	25	Fumigación periódica	31/07/2018	15/12/2018	Equipo de trabajo	
		La frecuencia de la ejecución del control y seguimiento es adecuada	15						
Recolección de aguas lluvias	Preventivo	¿El control es automático?	15	60	Control de los tanques de recolección de aguas lluvias	31/07/2018	15/12/2018	Equipo de trabajo	
		La frecuencia de la ejecución del control y seguimiento es adecuada	15						
		En el tiempo definido que lleva la herramienta ha demostrado ser efectiva	30						
Estructura sismo resistente	Preventivo	¿El control es automático?	15	60	Verificación periódica de la infraestructura	31/07/2018	15/12/2018	Equipo de trabajo	
		La frecuencia de la ejecución del control y seguimiento es adecuada	15						
		En el tiempo definido que lleva la herramienta ha demostrado ser efectiva	30						
Para rayos	Preventivo	No existe control	0	0		31/07/2018	15/12/2018	Equipo de trabajo	

4. VALORACIÓN DEL RIESGO									
Controles existentes	Tipo de control	Criterios de valoración de control	Puntaje	Puntaje Final	Acciones de Mitigación				
					Acción de Mitigación	Fecha Inicio	Fecha Fin	Responsable	Indicador
Sensibilización de las políticas de seguridad	Preventivo	Existen manuales, instructivos o procedimientos para el manejo de la herramienta	15	25	Divulgación de las políticas de seguridad de la información	31/07/2018	15/12/2018	Equipo de trabajo	
		¿Se cuenta con evidencias de la ejecución y seguimiento del control?	10						
Sensibilización en buenas prácticas	Preventivo	No existe control	0	0	Programación de talleres en buenas prácticas	31/07/2018	15/12/2018	Equipo de trabajo	
Plan de capacitación en el manejo adecuado de la información	Preventivo	No existe control	0	0	Plan de capacitaciones en el manejo adecuado de la información	31/07/2018	15/12/2018	Equipo de trabajo	
Plan de mantenimiento	Preventivo	No existe control	0	0	Solicitud a Redp, de mantenimiento periódico.	31/07/2018	15/12/2018	Equipo de trabajo	
Verificación periódica de inventarios de equipos	Preventivo	¿El control es manual?	10	55	Verificación periódica de inventarios de equipos	31/07/2018	15/12/2018	Equipo de trabajo	
		La frecuencia de la ejecución del control y seguimiento es adecuada	15						
		En el tiempo definido que lleva la herramienta ha demostrado ser efectiva	30						
Dar a conocer los protocolos existentes en el manejo de equipos	Preventivo	No existe control	0	0	Diseñar y dar a conocer los protocolos en el manejo de equipos	31/07/2018	15/12/2018	Equipo de trabajo	
Capacitación del personal frente a la protección	Preventivo	No existe control	0	0	Plan de capacitaciones en el tema de protección	31/07/2018	15/12/2018	Equipo de trabajo	
Actualización de antivirus	Preventivo	¿El control es automático?	15	60	Solicitar a Redp actualizaciones periódicas de los antivirus.	31/07/2018	15/12/2018	Equipo de trabajo	
		La frecuencia de la ejecución del control y seguimiento es adecuada	15						

4. VALORACIÓN DEL RIESGO									
Controles existentes	Tipo de control	Criterios de valoración de control	Puntaje	Puntaje Final	Acciones de Mitigación				
					Acción de Mitigación	Fecha Inicio	Fecha Fin	Responsable	Indicador
		En el tiempo definido que lleva la herramienta ha demostrado ser efectiva	30						
Talleres de sensibilización para identificar posibles ataques	Preventivo	No existe control	0	0	Programa de sensibilización para identificar posibles ataques	31/07/2018	15/12/2018	Equipo de trabajo	

Fuente el autor.

Teniendo en cuenta el alcance definido en el SGSI de la institución, el cual abarca todos los activos de la información y manejo de datos involucrados en la gestión de archivo de los procesos institucionales, en la tabla 24 se relacionan los activos con nivel de criticidad valorado en alto y medio a los cuales se aplicaran las acciones que mitiguen las consecuencias de los riesgos.

Tabla 24. Inventario de activos de información.

No.	Tipo de Activo	Nombre del activo	Ubicación	Criticidad	Soporte
1	[D]	Correspondencia enviada y recibida de almacén	Almacén	Alto	Físico
2	[D]	Formato de traslados de elementos	Almacén	Alto	Físico
3	[D]	Formatos de bienes y bajas	Almacén	Alto	Físico
4	[D]	Formatos de entradas y salidas de almacén	Almacén	Alto	Físico
5	[D]	Inventarios por dependencia	Almacén	Alto	Físico
6	[D]	Actas de reuniones de biblioteca.	Biblioteca	Alto	Físico
7	[D]	Informes de biblioteca	Biblioteca	Alto	Digital
8	[D]	Inventario de existencias de la biblioteca	Biblioteca	Alto	Digital
9	[D]	Plan anual de actividades de la biblioteca	Biblioteca	Alto	Digital
10	[D]	Planillas de préstamo de libros	Biblioteca	Alto	Físico
11	[D]	Plantillas de actividades de préstamo de cajas viajeras y de tablets	Biblioteca	Alto	Físico
12	[D]	Actas de reunión de coordinación	Coordinación	Alto	Físico
13	[D]	Actas de reunión por áreas o ciclos.	Coordinación	Alto	Físico
14	[D]	Compromisos convivenciales	Coordinación	Alto	Digital
15	[D]	Consolidados de notas de estudiantes	Coordinación	Alto	Físico
16	[D]	Observadores de estudiantes	Coordinación	Alto	Físico
17	[D]	Planes de estudio de todas las áreas	Coordinación	Alto	Físico
18	[D]	Remisiones a Comité de convivencia	Coordinación	Alto	Físico
19	[D]	Unidades temáticas de todas las áreas	Coordinación	Alto	Físico

No.	Tipo de Activo	Nombre del activo	Ubicación	Criticidad	Soporte
20	[D]	Registro fotográfico de actividades académicas	Docentes	Alto	Digital
21	[D]	Remisiones de estudiantes a orientación	Docentes	Alto	Físico
22	[D]	Actas auxiliares de enfermería	Docentes de EE	Alto	Físico
23	[D]	Actas de reunión de educación especial	Docentes de EE	Alto	Físico
24	[D]	Boletines anexos de estudiantes con NEE	Docentes de EE	Alto	Físico
25	[D]	Diagnósticos de los estudiantes con NEE	Docentes de EE	Alto	Físico
26	[D]	Formato de flexibilización para estudiantes con NEE	Docentes de EE	Alto	Físico
27	[D]	Informes de comisión de evaluación de estudiantes con NEE	Docentes de EE	Alto	Físico
28	[D]	Acta de compromiso de servicio social	Orientación escolar	Alto	Físico
29	[D]	Actas de reunión de orientación escolar	Orientación escolar	Alto	Físico
30	[D]	Asistencia al servicio social	Orientación escolar	Alto	Físico
31	[D]	Certificados de servicio social	Orientación escolar	Alto	Físico
32	[D]	Evaluación del Servicio Social	Orientación escolar	Alto	Físico
33	[D]	Formato de atención individual a estudiantes	Orientación escolar	Alto	Físico
34	[D]	Remisión de estudiantes a la EPS	Orientación escolar	Alto	Físico
35	[D]	Remisión de estudiantes por parte de los docente	Orientación escolar	Alto	Físico
36	[D]	Remisión de necesidades educativas especiales - NEE	Orientación escolar	Alto	Físico
37	[D]	Actas de arqueo	Pagaduría	Alto	Físico
38	[D]	Cargue información Contraloría	Pagaduría	Alto	Físico
39	[D]	Cargue información Contribución	Pagaduría	Alto	Físico
40	[D]	Cargue información presupuestal MEN	Pagaduría	Alto	Físico
41	[D]	Cargue información presupuestal SED	Pagaduría	Alto	Físico
42	[D]	Cierre de tesorería	Pagaduría	Alto	Físico
43	[D]	Comprobantes de ingreso	Pagaduría	Alto	Físico
44	[D]	Conciliaciones bancarias diferentes cuentas bancarias	Pagaduría	Alto	Físico
45	[D]	Contrato de acuerdo a las necesidades y obligaciones contraídas por la institución.	Pagaduría	Alto	Físico
46	[D]	Contrato de arrendamiento espacio tienda escolar	Pagaduría	Alto	Físico
47	[D]	Correspondencia enviada y recibida de pagaduría	Pagaduría	Alto	Físico
48	[D]	Extractos bancarios	Pagaduría	Alto	Físico
49	[D]	Formularios de pago reteica	Pagaduría	Alto	Físico
50	[D]	Formularios pago de estampilla	Pagaduría	Alto	Físico
51	[D]	Formularios pago de retefuente	Pagaduría	Alto	Físico
52	[D]	Informe base de retefuente	Pagaduría	Alto	Físico
53	[D]	Informe base retención reteica	Pagaduría	Alto	Físico
54	[D]	Informes Consejo Directivo	Pagaduría	Alto	Físico

No.	Tipo de Activo	Nombre del activo	Ubicación	Criticidad	Soporte
55	[D]	Libros de bancos cuentas bancarias	Pagaduría	Alto	Físico
56	[D]	Soportes ingresos	Pagaduría	Alto	Físico
57	[D]	Traslados bancarios	Pagaduría	Alto	Físico
58	[D]	Estrategias institucionales	Rectoría	Alto	Físico
59	[D]	Formulación del MECI	Rectoría	Alto	Físico
60	[D]	Formulación del PEI	Rectoría	Alto	Físico
61	[D]	Formulación del POA	Rectoría	Alto	Físico
62	[D]	Formulación del SIEE	Rectoría	Alto	Físico
63	[D]	Pacto de convivencia	Rectoría	Alto	Físico
64	[D]	Proyecto de síntesis	Docentes	Alto	Digital
65	[D]	Actas de comisión de evaluación y promoción	Secretaría académica	Alto	Físico
66	[D]	Actas de retiro de estudiantes	Secretaría académica	Alto	Físico
67	[D]	Actualización de datos	Secretaría académica	Alto	Físico
68	[D]	Auditorías académicas	Secretaría académica	Alto	Digital
69	[D]	Constancias y certificados	Secretaría académica	Alto	Digital
70	[D]	Continuidad y Promoción	Secretaría académica	Alto	Digital
71	[D]	Documentos de estudiantes activos.	Secretaría académica	Alto	Físico
72	[D]	Documentos de estudiantes retirados por inasistencia	Secretaría académica	Alto	Físico
73	[D]	Grados de bachilleres	Secretaría académica	Alto	Digital
74	[D]	Informe del DANE	Secretaría académica	Alto	Digital
75	[D]	Libro de grados.	Secretaría académica	Alto	Físico
76	[D]	Libro de valoración académica	Secretaría académica	Alto	Físico
77	[D]	Actas de Comité de compras	Secretaría de rectoría	Alto	Físico
78	[D]	Actas de Comité de mantenimiento	Secretaría de rectoría	Alto	Físico
79	[D]	Actas de Comité de sostenibilidad	Secretaría de rectoría	Alto	Físico
80	[D]	Actas de Comité de tienda escolar	Secretaría de rectoría	Alto	Físico
81	[D]	Actas de Consejo Académico	Secretaría de rectoría	Alto	Digital
82	[D]	Actas de Consejo Directivo	Secretaría de rectoría	Alto	Físico
83	[D]	Ausentismo	Secretaría de rectoría	Alto	Digital
84	[D]	Correspondencia externa enviada de rectoría	Secretaría de rectoría	Alto	Físico
85	[D]	Correspondencia externa recibida de rectoría	Secretaría de rectoría	Alto	Físico
86	[D]	Correspondencia interna enviada de rectoría	Secretaría de rectoría	Alto	Físico
87	[D]	Correspondencia interna recibida de rectoría	Secretaría de rectoría	Alto	Físico
88	[D]	Directorio de docentes	Secretaría de rectoría	Alto	Digital
89	[D]	Evaluación docentes	Secretaría de rectoría	Alto	Digital
90	[D]	Evaluación Sra. Rectora	Secretaría de rectoría	Alto	Digital
91	[D]	Hojas de vidas de docentes	Secretaría de rectoría	Alto	Físico
92	[D]	Horas extras	Secretaría de rectoría	Alto	Físico
93	[D]	Incapacidades	Secretaría de rectoría	Alto	Físico

No.	Tipo de Activo	Nombre del activo	Ubicación	Criticidad	Soporte
94	[D]	Informe de Contraloría	Secretaría de rectoría	Alto	Digital
95	[D]	Informe del DANE de docentes	Secretaría de rectoría	Alto	Digital
96	[D]	Mapa de Riesgos	Secretaría de rectoría	Alto	Digital
97	[D]	POA	Secretaría de rectoría	Alto	Digital
98	[D]	PQR	Secretaría de rectoría	Alto	Físico
99	[D]	Radicados	Secretaría de rectoría	Alto	Digital
100	[D]	Resoluciones de rectoría	Secretaría de rectoría	Alto	Digital
101	[D]	Semanario	Secretaría de rectoría	Alto	Digital
102	[D]	Encuentros literarios	Biblioteca	Medio	Físico
103	[D]	Recomendaciones culturales	Biblioteca	Medio	Digital
104	[D]	Talleres literarios	Biblioteca	Medio	Físico
105	[D]	Unidades didácticas	Biblioteca	Medio	Digital
106	[D]	Control de asistencia de docentes	Coordinación	Medio	Físico
107	[D]	Control de asistencia de estudiantes	Coordinación	Medio	Digital
108	[D]	Directorio de estudiantes	Coordinación	Medio	Físico
109	[D]	Docentes representantes al consejo académico	Coordinación	Medio	Físico
110	[D]	Docentes representantes al consejo directivo	Coordinación	Medio	Físico
111	[D]	Formatos de inscripción a media	Coordinación	Medio	Digital
112	[D]	Metodologías de trabajo de las áreas	Coordinación	Medio	Físico
113	[D]	Padres representantes a gobierno escolar	Coordinación	Medio	Digital
114	[D]	Salida de estudiantes	Coordinación	Medio	Físico
115	[D]	Formato de reunión con docentes de estudiantes con NEE	Docentes de EE	Medio	Físico
116	[D]	Formato de reunión con padres de estudiantes con NEE	Docentes de EE	Medio	Físico
117	[D]	Formato de seguimiento de estudiantes con NEE	Docentes de EE	Medio	Físico
118	[D]	Valoraciones pedagógicas	Docentes de EE	Medio	Físico
119	[D]	Asistencia a escuela de padres, talleres estudiantes	Orientación escolar	Medio	Físico
120	[D]	Acuerdos	Pagaduría	Medio	Físico
121	[D]	Necesidades por áreas	Pagaduría	Medio	Físico
122	[D]	Plan de adquisiciones y compras	Pagaduría	Medio	Físico
123	[D]	Proyecto presupuestal	Pagaduría	Medio	Físico
124	[D]	Proyectos institucionales	Pagaduría	Medio	Físico
125	[D]	Lineamientos presupuestales	Pagaduría	Medio	Físico
126	[D]	Cronograma institucional anual	Rectoría	Medio	Físico
127	[D]	Material de apoyo	Docentes	Medio	Físico
128	[D]	Organización cátedra por la paz	Docentes	Medio	Digital
129	[D]	Talleres	Docentes	Medio	Digital
130	[D]	Turnos de acompañamiento	Docentes	Medio	Físico
131	[D]	Archivo inactivo	Secretaría académica	Medio	Digital
132	[D]	Documentos para grado.	Secretaría académica	Medio	Físico

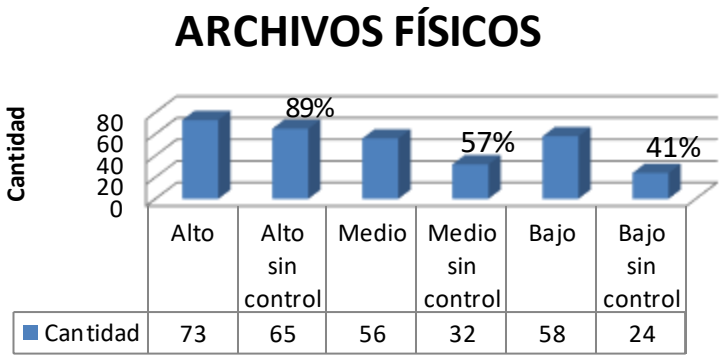
No.	Tipo de Activo	Nombre del activo	Ubicación	Criticidad	Soporte
133	[D]	Estadísticas secretaría académica	Secretaría académica	Medio	Digital
134	[D]	Informes a Pagaduría	Secretaría académica	Medio	Digital
135	[D]	Listados de auditorías	Secretaría académica	Medio	Físico
136	[D]	Listados de estudiantes por cursos y jornadas	Secretaría académica	Medio	Digital
137	[D]	Matrículas	Secretaría académica	Medio	Digital
138	[D]	Movilidad escolar	Secretaría académica	Medio	Físico
139	[D]	Novedades del sistema de apoyo escolar	Secretaría académica	Medio	Físico
140	[D]	Oficios elaborados	Secretaría académica	Medio	Digital
141	[D]	Proyección	Secretaría académica	Medio	Digital
142	[D]	Solicitudes de padres de familia.	Secretaría académica	Medio	Físico
143	[D]	Solicitudes enviadas	Secretaría académica	Medio	Físico
144	[D]	Solicitudes recibidas	Secretaría académica	Medio	Físico
145	[D]	Subsidios condicionados	Secretaría académica	Medio	Digital
146	[D]	Coordinadores	Secretaría de rectoría	Medio	Digital
147	[D]	Correos electrónicos	Secretaría de rectoría	Medio	Físico
148	[D]	Diplomado rectores	Secretaría de rectoría	Medio	Digital
149	[D]	Formatos de permisos	Secretaría de rectoría	Medio	Físico
150	[D]	Formatos Institucionales	Secretaría de rectoría	Medio	Físico
151	[D]	Hojas control de expedientes archivo inactivo	Secretaría de rectoría	Medio	Físico
152	[D]	Inventario documental del archivo inactivo	Secretaría de rectoría	Medio	Físico
153	[D]	Varios	Secretaría de rectoría	Medio	Físico
154	[HW]	Equipo de cómputo del almacén	Almacén	Alto	Físico
155	[HW]	Equipo de cómputo de la biblioteca	Biblioteca	Alto	Físico
156	[HW]	Equipo de cómputo coordinación académica	Coordinación	Alto	Físico
157	[HW]	Equipo de cómputo coordinación de convivencia	Coordinación	Alto	Físico
158	[HW]	Equipo de cómputo coordinación de media fortalecida	Coordinación	Alto	Físico
159	[HW]	Equipo de cómputo de pagaduría	Pagaduría	Alto	Físico
160	[HW]	Equipo de cómputo de rectoría	Rectoría	Alto	Físico
161	[HW]	Equipo de cómputo de secretaria académica	Secretaría académica	Alto	Físico
162	[HW]	Equipo de cómputo de secretaria de rectoría	Secretaría de rectoría	Alto	Físico
163	[SW]	Ficha de referenciación y autorización de contacto línea psicoactiva.	Orientación escolar	Alto	Digital
164	[SW]	Sistema de alertas de la Secretaria Educación Distrital	Orientación escolar	Alto	Digital
165	[SW]	Aplicativo de verificación de asistencia	Aplicación web	Alto	Digital
166	[SW]	Sistema integrado de gestión documental y archivo SIGA	Aplicación web	Alto	Digital
167	[SW]	Sistema de matrícula SIMAT	Aplicación web	Alto	Digital

No.	Tipo de Activo	Nombre del activo	Ubicación	Criticidad	Soporte
168	[SW]	Sistema Biométrico del Colegio Germán Arciniegas	Secretaría académica	Alto	Digital

Fuente: el autor.

En la clasificación de los activos físicos se determinó el nivel de criticidad basado en los factores de confidencialidad, integridad y disponibilidad; evidenciando la carencia de controles en aquellos activos que son importantes en la institución, dado que el 89% de los archivos considerados con un nivel de criticidad alta, no cuenta con ningún tipo de control al igual que el 57% de los archivos físicos con nivel de criticidad medio, como se observa en la figura 21.

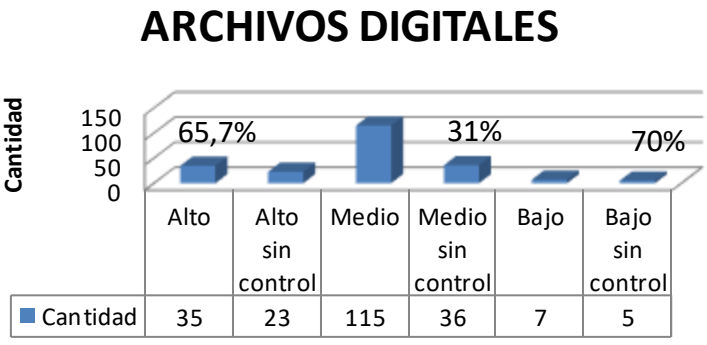
Figura 21. Archivos físicos sin controles.



Fuente el autor.

Adicionalmente, en la clasificación de los activos digitales se determinó el nivel de criticidad basado en los factores de confidencialidad, integridad y disponibilidad; evidenciando que el 65,7% de los archivos considerados con un nivel de criticidad alta no cuenta con ningún tipo de control al igual que el 31% de los archivos físicos con nivel de criticidad medio, como se observa en la figura 22.

Figura 22. Archivos digitales sin controles.



Fuente el autor.

7.3.3. Definición de controles y acciones.

En el colegio Germán Arciniegas IED, se realizó la valoración de los controles definidos en el Anexo A de la norma NTC ISO/IEC 27001:2013, donde se identificó si se cumplen total o parcial los controles definidos en este anexo o si no se cumplen estos, como se evidencia en la tabla 25.

Tabla 25. Controles del Anexo A de la NTC ISO/IEC 27001:2013.

Controles			Cumple			Observaciones
			Si	No	Parcial	
5. Políticas de la seguridad de la información	5.1. Orientación de la dirección para la gestión de la seguridad de la información	5.1.1. Políticas para la seguridad de la información	X			
		5.1.2. Revisión de las políticas para seguridad de la información	X			
6. Organización de la seguridad de la información	6.1. Organización interna	6.1.1. Roles y responsabilidades para la seguridad de información			X	
		6.1.2. Separación de deberes				Administrado por la SED.
		6.1.3. Contacto con las autoridades			X	
		6.1.4. Contacto con grupos de interés especial		X		
		6.1.5. Seguridad de la información en la gestión de proyectos			X	
	6.2. Dispositivos móviles y teletrabajo	6.2.1.Política para dispositivos móviles				Administrado por la SED.
		6.2.2.Teletrabajo				Administrado por la SED.
7. Seguridad de los recursos humanos	7.1. Antes de asumir el empleo	7.1.1. Selección				Administrado por la SED.
		7.1.2.Términos y condiciones del empleo				Administrado por la SED.
	7.2. Durante la ejecución del empleo	7.2.1. Responsabilidades de la dirección	X			
		7.2.2. Toma de conciencia, educación y formación en la seguridad de la información	X			
		7.2.3. Proceso disciplinario			X	
	7.3. Terminación y cambio de empleo	7.3.1. Terminación o cambio de responsabilidades de empleo	X			
8. Gestión de activos	8.1. Responsabilidad por los activos	8.1.1. Inventario de activos	X			
		8.1.2. Propiedad de los activos	X			
		8.1.3. Uso aceptable de los activos			X	
		8.1.4. Devolución de activos	X			

Controles			Cumple			Observaciones
			Si	No	Parcial	
	8.2. Clasificación de la información	8.2.1. Clasificación de la información	X			
		8.2.2. Etiquetado de la información			X	
		8.2.3. Manejo de activos			X	
	8.3. Manejo de medios	8.3.1. Gestión de medios removibles			X	
		8.3.2 . Disposición de los medios			X	
		8.3.3. Transferencia de medios físicos			X	
9. Control de acceso	9.1. Requisitos del negocio para control de acceso	9.1.1. Política de control de acceso	X			
		9.1.2. Acceso a redes y a servicios en red	X			
	9.2. Gestión de acceso de usuarios	9.2.1. Registro y cancelación del registro de usuarios	X			
		9.2.2. Suministro de acceso de usuarios	X			
		9.2.3. Gestión de derechos de acceso privilegiado	X			
		9.2.4. Gestión de información de autenticación secreta de usuarios	X			
		9.2.5. Revisión de los derechos de acceso de usuarios	X			
		9.2.6. Retiro o ajuste de los derechos de acceso	X			
	9.3. Responsabilidades de los usuarios	9.3.1. Uso de la información de autenticación secreta			X	
	9.4. Control de acceso a sistemas y aplicaciones	9.4.1. Restricción de acceso Información			X	
		9.4.2. Procedimiento de ingreso seguro			X	
		9.4.3. Sistema de gestión de contraseñas			X	
		9.4.4. Uso de programas utilitarios privilegiados				Administrado por la SED.
		9.4.5. Control de acceso a códigos fuente de programas				Administrado por la SED.
10. Criptografía	10.1. Controles criptográficos	10.1.1. Política sobre el uso de controles criptográficos	X			
		10.1.2. Gestión de llaves	X			
11. Seguridad física y del entorno	11.1. Áreas seguras	11.1.1. Perímetro de seguridad física	X			
		11.1.2. Controles físicos de entrada	X			

Controles			Cumple			Observaciones
			Si	No	Parcial	
		11.1.3. Seguridad de oficinas, recintos e instalaciones			X	
		11.1.4. Protección contra amenazas externas y ambientales			X	
		11.1.5. Trabajo en áreas seguras			X	
		11.1.6. Áreas de despacho y carga			X	
	11.2. Equipos	11.2.1. Ubicación y protección de los equipos	X			
		11.2.2. Servicios de suministro	X			
		11.2.3. Seguridad del cableado	X			
		11.2.4. Mantenimiento de equipos			X	
		11.2.5. Retiro de activos	X			
		11.2.6. Seguridad de equipos y activos fuera de las instalaciones	X			
		11.2.7. Disposición segura o reutilización de equipos			X	
		11.2.8. Equipos de usuario desatendidos			X	
		11.2.9. Política de escritorio limpio y pantalla limpia			X	
12. Seguridad de las operaciones	12.1. Procedimientos operacionales y responsabilidades	12.1.1. Procedimientos de operación documentados			X	
		12.1.2. Gestión de cambios			X	
		12.1.3. Gestión de capacidad			X	
		12.1.4. Separación de los ambientes de desarrollo, pruebas y operación			X	
	12.2. Protección contra códigos maliciosos	12.2.1. Controles contra códigos maliciosos			X	
	12.3. Copias de respaldo	12.3.1. Respaldo de información			X	
	12.4. Registro y seguimiento	12.4.1. Registro de eventos			X	
		12.4.2. Protección de la información de registro	X			
		12.4.3. Registros del administrador y del operador				Administrado por la SED.
		12.4.4. Sincronización de relojes	X			
	12.5. Control de software operacional	12.5.1. Instalación de software en sistemas operativos				Administrado por la SED.

Controles			Cumple			Observaciones
			Si	No	Parcial	
	12.6. Gestión de la vulnerabilidad técnica	12.6.1. Gestión de las vulnerabilidades técnicas			X	
		12.6.2. Restricciones sobre la instalación de software	X			Administrados por la SED.
	12.7. Consideraciones sobre auditorias de sistemas de información	12.7.1. Información controles de auditoría de sistemas			X	
13. Seguridad de las comunicaciones	13.1. Gestión de la seguridad de las redes	13.1.1. Controles de redes				Administrado por la SED.
		13.1.2. Seguridad de los servicios de red				Administrado por la SED.
		13.1.3. Separación en las redes				Administrado por la SED.
	13.2. Transferencia de información	13.2.1. Políticas y procedimientos de transferencia de información			X	
		13.2.2. Acuerdos sobre transferencia de información			X	
		13.2.3. Mensajería electrónica	X			
		13.2.4. Acuerdos de confidencialidad o de no divulgación	X			
14. Adquisición, desarrollo y mantenimientos de sistemas	14.1. Requisitos de seguridad de los sistemas de información	14.1.1. Análisis y especificación de requisitos de seguridad de la información			X	
		14.1.2. Seguridad de servicios de las aplicaciones en redes publicas				Administrado por la SED.
		14.1.3. Protección de transacciones de los servicios de las aplicaciones				Administrado por la SED.
	14.2. Seguridad en los procesos de desarrollo y de soporte	14.2.1. Política de desarrollo seguro				Administrado por la SED.
		14.2.2. Procedimientos de control de cambios en sistemas				Administrado por la SED.
		14.2.3. Revisión técnica de las aplicaciones después de cambios en la plataforma de operación				Administrado por la SED.
		14.2.4. Restricciones en los cambios a los paquetes de software				Administrado por la SED.
		14.2.5. Principios de construcción de sistemas seguros				Administrado por la SED.
		14.2.6. Ambiente de desarrollo seguro				Administrado por la SED.

Controles			Cumple			Observaciones
			Si	No	Parcial	
		14.2.7. Desarrollo contratado externamente				Administrado por la SED.
		14.2.8. Pruebas de seguridad de sistemas				Administrado por la SED.
		14.2.9. Prueba de aceptación de sistemas				Administrado por la SED.
	14.3. Datos de prueba	14.3.1. Protección de datos de prueba				Administrado por la SED.
15. Relación con los proveedores	15.1. Seguridad de la información en las relaciones con los proveedores	15.1.1. Política de seguridad de la información para las relaciones con proveedores	X			
		15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores	X			
		15.1.3. Cadena de suministro de tecnología de información y comunicación	X			
	15.2. Gestión de la prestación de servicios con los proveedores	15.2.1. Seguimiento y revisión de los servicios de los proveedores	X			
		15.2.2. Gestión de cambios en los servicios de proveedores	X			
16. Gestión de incidentes de seguridad de la información	16.1. Gestión de incidentes y mejoras en la seguridad de la información	16.1.1. Responsabilidad y procedimientos			X	
		16.1.2. Reporte de eventos de seguridad de la información			X	
		16.1.3. Reporte de debilidades de seguridad de la información			X	
		16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos			X	
		16.1.5. Respuesta a incidentes de seguridad de la información			X	
		16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información			X	
		16.1.7. Recolección de evidencia			X	
17. Aspectos de seguridad de la información de la gestión de continuidad de negocio	17.1. Continuidad de seguridad de la información	17.1.1. Planificación de la continuidad de la seguridad de la información			X	
		17.1.2. Implementación de la continuidad de la seguridad de la información			X	

Controles			Cumple			Observaciones
			Si	No	Parcial	
		17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información			X	
	17.2. Redundancias	17.2.1. Disponibilidad de instalaciones de procesamiento de información.		X		
18. Cumplimiento	18.1. Cumplimiento de requisitos legales y contractuales	18.1.1. Identificación de la legislación aplicable y de los requisitos contractuales	X			
		18.1.2. Derechos de propiedad intelectual	X			
		18.1.3. Protección de registros			X	
		18.1.4. Privacidad y protección de datos personales			X	
		18.1.5. Reglamentación de controles criptográficos	X			
	18.2. Revisiones de seguridad de la información	18.2.1. Revisión independiente de la seguridad de la información			X	
		18.2.2. Cumplimiento con las políticas y normas de seguridad			X	
		18.2.3. Revisión del cumplimiento técnico			X	

Fuente el autor.

De acuerdo con los resultados obtenidos con la verificación de controles, se planean las acciones a realizar, con el fin de brindar la seguridad de la información en la gestión de archivo del colegio Germán Arciniegas Institución Educativa Distrital. Estas acciones se encuentran a continuación en la tabla 26.

Tabla 26. Acciones de seguridad en los controles del Anexo A.

Controles	Observaciones
5. Políticas de la seguridad de la información	Falta divulgación de las políticas de seguridad en los funcionarios de la institución.
6. Organización de la seguridad de la información	Aunque hay roles y responsabilidades definidas, falta documentación.
	Falta obtener algunos contactos con las autoridades pertinentes.
	Se desconocen los grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
	Falta integrar la seguridad de la información en la gestión de proyectos institucionales.

Controles	Observaciones
7. Seguridad de los recursos humanos	La contratación de los funcionarios, se realiza desde el nivel central de la SED.
	No se cuenta con las directrices para el inicio de un proceso, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
8. Gestión de activos	Falta documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
	Falta diseñar los procedimientos para el etiquetado de la información con el esquema de clasificación de información adoptado por la IED.
	Falta desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con las directrices dadas por la SED.
	Falta definir los procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la IED.
	Los medios que contienen información que se deben proteger contra acceso no autorizado, uso indebido o corrupción, no son transportados fuera de la institución.
9. Control de acceso	Falta sensibilizar a los usuarios que cumplan con las prácticas de la organización para el uso de información de autenticación secreta.
	Falta sensibilización de la política de control de acceso e ingreso seguro.
	Falta sensibilización en el uso de contraseñas robustas.
10. Criptografía	Es administrada por la Secretaría de Educación del Distrito.
11. Seguridad física y del entorno	Faltan los protocolos de la seguridad física a oficinas, recintos e instalaciones.
	Falta definir procedimientos para trabajo en áreas seguras.
	Falta definir procedimientos para controlar el acceso a las áreas donde no pueden ingresar personal no autorizadas.
	Carece de un plan de mantenimiento de equipos.
	Faltan definir criterios para verificar los elementos de equipos que contengan medios de almacenamiento y que estos no hayan sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.
	Falta definir criterios para los equipos desatendidos y que se le brinde la protección apropiada.
	Falta concientización de la política de escritorio limpio y pantalla limpia en las instalaciones de procesamiento de información.
12. Seguridad de las operaciones	Falta divulgación de los procedimientos de operación.
	Falta diseñar formatos para el control de 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.
	Aunque se cuenta con la protección para el ingreso de intruso, falta concientización de los usuarios para la protección contra códigos maliciosos.
	Falta realiza copias de seguridad como respaldo de la información.

Controles	Observaciones
	Falta realizar registros de las actividades de usuarios, fallas y eventos de seguridad de la información.
	Falta revisión periódica que permita obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información y evaluar la exposición de la organización a estas vulnerabilidades con el fin de tomar las medidas apropiadas para tratamiento de los riesgos asociados.
	Aplicación de auditorías que permitan la verificación de los sistemas en los procesos institucionales.
13. Seguridad de las comunicaciones	Falta divulgar los procedimientos y controles definidos para la protección en la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.
14. Adquisición, desarrollo y mantenimientos de sistemas	Falta definir los requisitos de seguridad de la información que se deben incluir en los nuevos sistemas de información o para mejoras de los sistemas de información existentes.
15. Relación con los proveedores	Los procesos con los proveedores se realizan mediante aplicativo web implementado por la SED.
16. Gestión de incidentes de seguridad de la información	Falta establecer las responsabilidades y procedimientos de gestión para las respuestas a los incidentes de seguridad de la información, proceso de información y reporte de estos incidentes.
17. Aspectos de seguridad de la información de la gestión de continuidad de negocio	Falta definir criterios en la organización para mantener los procesos, procedimientos y controles que aseguren la continuidad de la seguridad de la información la IED.
18. Cumplimiento	Falta realizar la protección de la información contra daño, pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con la normatividad legal vigente.
	Falta definir los procesos y procedimientos en la protección de la información de datos personales.
	Definir la periodicidad de la revisión de los procesos y los procedimientos del SGSI del colegio, con el fin de tenerlos actualizados, así como el cumplimiento de las normas y políticas establecidas.

Fuente el autor.

El comité encargado del SGSI del colegio Germán Arciniegas, presentará a los funcionarios de la institución los informes, cambios, actualizaciones y demás información importante del sistema, en las semanas de planeación institucional previa programación con la rectora de la institución.

7.3.4. Objetivos de seguridad de la información y planes para lograrlos

Para el logro de los objetivos definidos en el sistema de gestión e seguridad de la información del Colegio Germán Arciniegas, se definen las actividades a desarrollar con los respectivos porcentajes en las metas y los resultados, como se evidencia en la tabla 27.

Tabla 27. Actividades para el logro de objetivos.

Objetivo 1 del SGSI del colegio Germán Arciniegas: Definir el contexto del colegio Germán Arciniegas, necesidades y expectativas de las partes interesadas.		
Actividades para el logro del objetivo	Meta	Resultado
Recolección de la información institucional existente.	5%	5%
Diseño de encuesta para la recolección de la información en las diferentes áreas de la institución en formulario web.	5%	5%
Presentación y aprobación de la propuesta de encuesta al equipo directivo de la institución.	5%	5%
Aplicación de la encuesta al personal del colegio Germán Arciniegas.	5%	5%
Consolidación de la información obtenida en la aplicación de la encuesta.	5%	5%
Total	25%	25%
Objetivo 2 del SGSI del colegio Germán Arciniegas: Determinar el alcance del sistema de gestión de seguridad de la información de la Institución Educativa Distrital.		
Actividades para el logro del objetivo	Meta	Resultado
Definición de la matriz DOFA de la IED.	12%	12%
Definición del alcance del SGSI del colegio.	13%	13%
Total	25%	25%
Objetivo 3 del SGSI del colegio Germán Arciniegas: Valorar los riesgos a los que se encuentra expuesta la información del colegio y definir acciones para tratar riesgos y oportunidades.		
Actividades para el logro del objetivo	Meta	Resultado
Consolidación del inventario de activos de la información del colegio Germán Arciniegas.	10%	10%
Clasificación de la información recolectada en la base de datos, según su nivel de importancia de acuerdo con los criterios de la SED.	5%	5%
Realización de la matriz de riesgos de la institución.	5%	5%
Análisis y tratamiento de los riesgos de la IED.	5%	5%
Total	25%	25%
Objetivo 4 del SGSI del colegio Germán Arciniegas: Definir los procesos y controles para la seguridad de la información que garanticen la disponibilidad, confiabilidad, e integridad de la información de la institución.		
Actividades para el logro del objetivo	Meta	Resultado
Identificación de los controles existentes en la institución.	5%	5%
Definición de controles a aplicar en el manejo de la información del colegio Germán Arciniegas.	10%	10%
Diseño del plan de comunicación y sensibilización en el personal de la IED.	5%	5%
Definición de los medios para la divulgación de la información del SGSI del colegio.	5%	5%
Total	25%	25%

Fuente el autor

7.3.5. Indicadores de gestión

Para la evidencia de los avances y el cumplimiento de los objetivos propuestos en el sistema, se han definido los siguientes indicadores de gestión que permitan medir la efectividad, eficacia y eficiencia del Sistema de Gestión de Seguridad de la Información del colegio Germán Arciniegas y el cumplimiento de los objetivos. Estos indicadores están relacionados en las tablas 28 y 29.

Tabla 28. Indicador de políticas de seguridad.

<table>
<tr><td colspan="3">INDICADOR 01- POLÍTICAS DE SEGURIDAD.</td></tr>
<tr><td colspan="3">DEFINICIÓN: El indicador permite determinar y hacer seguimiento al compromiso de la dirección, en cuanto a la divulgación y sensibilización de las políticas de seguridad de la información.</td></tr>
<tr><td colspan="3">OBJETIVO: Identificar si el personal de la institución tiene conocimiento y claridad de las políticas de seguridad definidas por la Secretaría de Educación del Distrito.</td></tr>
<tr><td>DESCRIPCIÓN DE VARIABLES</td><td>FORMULA</td><td>FUENTE DE INFORMACIÓN</td></tr>
<tr><td>VSI01: Número de funcionarios de la institución.</td><td rowspan="2">(VSI01/VSI02)*100</td><td>Encuestas aplicadas al personal de la IED.</td></tr>
<tr><td>VSI02: Número de personas con conocimiento y claridad de las políticas de seguridad de la información.</td><td></td></tr>
<tr><td colspan="3">METAS</td></tr>
<tr><td>MÍNIMA</td><td>SATISFACTORIA</td><td>SOBRESALIENTE</td></tr>
<tr><td>75-80%</td><td>80- 90%</td><td>100%</td></tr>
<tr><td colspan="3">OBSERVACIONES</td></tr>
<tr><td colspan="3">Para dar a conocer las políticas de seguridad de la información, es necesario definir un plan de capacitaciones al personal de la institución, la divulgación de estas mediante correo electrónico y publicación en el portal web.</td></tr>
</table>

Fuente el autor.

Tabla 29. Indicador del seguimiento a la seguridad de las operaciones.

<table>
<tr><td>INDICADOR 02 – SEGUIMIENTO A LA SEGURIDAD DE LAS OPERACIONES.</td></tr>
<tr><td>DEFINICIÓN: El indicador permite realizar el seguimiento a la seguridad en las operaciones y realización de las copias de respaldo.</td></tr>
<tr><td>OBJETIVO: Identificar el porcentaje de respaldo y seguridad en los activos informáticos.</td></tr>
</table>

DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
VSI01: Número de activos informáticos sin respaldo.	(VSI01/VSI02)*100	Matriz de activos de la información.
VSI02: Número de activos informáticos con respaldo.		Verificación de los activos que se encuentran con respaldos de seguridad.
METAS		
MÍNIMA	SATISFACTORIA	SOBRESALIENTE
75-80%	80- 90%	100%
OBSERVACIONES		
Para identificar el porcentaje de activos de la información que cuentan con respaldo, es necesario contar con un formato de seguimiento a las copias de seguridad y digitalización de la información.		

Fuente el autor.

7.4. SOPORTE

7.4.1. Recursos

Talento humano

A continuación se relacionan los proponentes que intervienen en el desarrollo del diseño del sistema de gestión de seguridad de la información para el colegio Germán Arciniegas IED:

- Ing. Gabriel Mauricio Ramírez Villegas, Director del proyecto de grado.
- Ing. Carolina Figueroa Cubillos, alumna investigadora.
- Dra. Sorangela Miranda Beltrán, Rectora del colegio Germán Arciniegas.

Recursos técnicos y materiales

Para el diseño del SGSI del colegio Germán Arciniegas, se han utilizado los siguientes equipos y materiales:

- ✓ Computador de escritorio
- ✓ Computador portátil
- ✓ Red de internet
- ✓ Fotocopiadora
- ✓ Útiles de oficina

Recursos económicos

Los costos para el desarrollo del diseño del sistema de gestión de seguridad de la información para el colegio Germán Arciniegas, como mínimo son por un valor de $ 565.000, los cuales se detallan a continuación en la tabla 30.

Tabla 30. Costos del desarrollo del proyecto.

Concepto	Ingresos	Egresos
Compra de la NTC-ISO-IEC 27001 – Sistemas de gestión de la seguridad de la información. Requisitos.		$ 67.000
Compra de la NTC-ISO-IEC 27002 – Código de práctica para controles de seguridad de la información.		$ 116.000
Compra de la NTC-ISO-IEC 27003 – Guía de implementación de un sistema de gestión de la seguridad de la información.		$ 116.000
Compra de la GTC-ISO-IEC 27035 – Gestión del riesgo en la seguridad de la información.		$ 116.000
Software para la administración del SGSI		
Transportes.		$ 50.000
Útiles, fotocopias y papelería en general.		$ 50.000
Varios.		$ 50.000
Total		$ 565.000

Fuente el autor.

7.4.2. Competencia

7.4.3. Toma de conciencia

Es necesario que el personal de la institución y la comunidad educativa en general, tome conciencia de los elementos que forman parte importante en el SGSI del colegio Germán Arciniegas, apliquen las Políticas de seguridad de la información adoptadas por la Secretaría de Educación del Distrito mediante la Resolución 1944 del 27 de octubre de 2016 y tengan conocimiento de las consecuencias de las no conformidades del gestión de gestión de la seguridad de la información del colegio.

7.4.4. Comunicación

El equipo de trabajo realiza el plan de comunicaciones que se evidencia en la tabla 31, con el fin de dar a conocer el Sistema de Gestión de seguridad de la Información del colegio Germán Arciniegas, su importancia, sus etapas y avances, mediante talleres de sensibilización a los diferentes grupos de interés que conforman la comunidad educativa. La información será transmitida mediante talleres, semanario, correo electrónico y publicación en la página web.

Tabla 31. Plan de comunicaciones.

Grupo de interés	Contenido del mensaje	Medio	Tiempo					
			Septiembre	Septiembre	Septiembre	Octubre	Octubre	Octubre
Equipo docente	Información general del SGSI y sus etapas. Políticas y uso del correo electrónico. Ley 1273 de 2009.	Presentación en Power Point. Información enviada por correo electrónico.	X					
Equipo directivo	Información general del SGSI y sus etapas. Políticas y uso del correo electrónico. Ley 1273 de 2009.	Presentación en Power Point. Información enviada por correo electrónico.				X		
Equipo administrativo	Información general del SGSI y sus etapas. Políticas y uso del correo electrónico. Ley 1273 de 2009.	Presentación en Power Point. Información enviada por correo electrónico.				X		
Consejo estudiantil	Información general del SGSI y sus etapas. Ley 1273 de 2009.	Presentación en Power Point. Información enviada por correo electrónico. Videos					X	
Consejo de padres	Información general del SGSI y sus etapas. Ley 1273 de 2009.	Presentación en Power Point. Información enviada por correo electrónico. Videos					X	
Consejo directivo	Información general del SGSI y sus etapas. Ley 1273 de 2009.	Presentación en Power Point. Información enviada por correo electrónico.						X

Fuente el autor.

7.4.5. Información documentada

En estos espacios denominados talleres de formación dirigidos a los diferentes grupos focales de la comunidad educativa (Directivos docentes, docentes, personal administrativo, estudiantes y padres de familia), se presentaran las generalidades del SGSI, las políticas de seguridad de la información dadas por la Secretaría de Educación del Distrito mediante Resolución No. 1944 del 27 de

octubre de 2016, normatividad vigente, procesos virtualizados, sensibilización del manejo de la información y redes sociales.

Con cada uno de estos grupos focales, se registrará mediante planillas de asistencia el personal capacitado, adicionalmente se llevarán a cabo evaluaciones de las diferentes capacitaciones, con el fin de verificar los indicadores de gestión y los resultados en términos de la apropiación de la iniciativa y su conceptualización por parte de la Comunidad Educativa.

INFOGRAFÍA


SGSI PARA EL COLEGIO GERMÁN ARCINIEGAS IED
ISO 27000
Diseñar el SGSI para el Colegio Germán Arciniegas I.E.D., bajo la norma técnica colombiana NTC-ISO-IEC 27001:2013.
1 RECOLECCIÓN DE LA INFORMACIÓN
Mediante la aplicación de encuesta web a todo el personal de la IED, se realiza la recolección de la información.
2 INVENTARIO DE ACTIVOS
Clasificación de la información y elaboración del inventario de activos de la información.
3 DEFINICIÓN DEL ALCANCE
ALCANCE
De la información recolectada, se delimitó el alcance del SGSI .
4 VALORACIÓN Y CLASIFICACIÓN DE LOS ACTIVOS
De acuerdo con la clasificación dada a los activos en los factores de confidencialidad, integridad y disponibilidad, se determinó el nivel de criticidad.
5 IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS
Se realiza la matriz de riesgos donde identificaron los riesgos, las consecuencias, la probabilidad de ocurrencia y evaluación del impacto.
6 ACCIONES DE MITIGACIÓN
Teniendo en cuenta la matriz de riesgos, se identifican los controles aplicados a los activos de la información y se definen las diferentes acciones para mitigar los impactos de ocurrencia.
7 PLAN DE ACCIONES
Se realiza un plan para iniciar el proceso de sensibilización y aplicación de controles con el personal de la institución.
8 IMPLEMENTACIÓN
El proyecto será presentado ante la Secretaría de Educación del Distrito, para su implementación.

CONCLUSIONES

Dado que la información es uno de los activos más importantes al interior de las organizaciones porque son parte fundamental en la toma de decisiones, en la medida en que se realizan ejercicios de gestión en este ámbito, es posible consolidar los demás aspectos que implica la administración eficaz y eficiente de una entidad; por lo tanto la información generada y tramitada en las oficinas del colegio Germán Arciniegas I.E.D., se consolida como fundamental para el desarrollo de las actividades académicas, de construcción de ciudadanía y administrativo-presupuestales propias de la Institución que permiten contribuir en la calidad de los procesos.

En razón a lo expuesto, se realiza el diseño del sistema de gestión de seguridad de la información, bajo la norma técnica colombiana NTC-ISO-IEC 27001:2013, para el Colegio Germán Arciniegas Institución Educativa Distrital (I.E.D.) basado en las normas legales vigentes, que permite el aseguramiento y estandarización de la información, garantizando la integridad, la conservación y organización de la misma.

Adicionalmente, se definió el contexto del colegio Germán Arciniegas, las necesidades y expectativas de las partes interesadas, involucrando de esta manera cada uno de los grupos focales de la comunidad educativa, como son el personal docente, directivo, administrativo, padres de familia y estudiantes. Adicionalmente, se determinó el alcance del sistema de gestión de seguridad de la información de la Institución Educativa Distrital.

Se levantó el inventario de activos de la información como el insumo más importante para el desarrollos del SGSI del colegio Germán Arciniegas, logrando esto con el apoyo de todo el personal docente, administrativo y directivo de la institución, quienes aportaron desde su área de conocimiento la información requerida para la clasificación de los activos.

De acuerdo con la clasificación dada a los activos informáticos, en los factores de confidencialidad, integridad y disponibilidad, se determinó el nivel de criticidad y los controles aplicados a estos activos, evidenciando la carencia de controles, dado que en un alto porcentaje de los archivos físicos y digitales no se cuenta con ningún tipo de control que mitigue el impacto en caso de que ocurra un evento negativo.

Una vez identificados los activos de la información de la IED, se identificaron y valoraron los riesgos a los que se encuentra expuesta la información del colegio, se definieron los planes de acción para tratarlos, procesos y controles para la seguridad de la información garantizando la disponibilidad, confiabilidad, e integridad de la información de la institución; donde el personal autorizado del colegio (docentes, directivos o administrativos), pueden consultar y acceder a ella

de manera ordenada, segura y controlada, salvaguardando los datos y su confidencialidad.

Aunque en el colegio Germán Arciniegas no se han presentado eventos negativos que generen acciones correctivas, se determinó la importancia de generar e implementar controles preventivos que mitiguen el impacto en caso de la materialización de una amenaza, dado que el estado de vulnerabilidad al que se encuentra expuesta la información de la institución educativa es muy alto.

Para el desarrollo de este documento se ha recopilado detalladamente la información de la Institución Educativa Distrital, utilizando los formatos y procedimientos establecidos por la Secretaría de Educación, con el fin de ser un documento base para el sistema de gestión de seguridad de la información del nivel institucional de la SED, es decir, que pueda ser un documento de referencia para las 362 Instituciones Educativas Distritales de la Secretaría de Educación de Bogotá y apoyo para la creación de protocolos del almacenamiento de la información.

Este trabajo representa el aporte a la excelencia germanista que desde el PEI institucional se aborda como esencia de todos los procesos y desde el ámbito de la gestión proyecta la relevancia de las acciones de los equipos administrativos en construir cultura institucional en el camino de la calidad.

Este proyecto se presentó ante la Secretaría de Educación del Distrito y las directivas del colegio Germán Arciniegas para su implementación y se ha aprobado esta implementación para el año 2019. En la implementación del sistema de gestión de seguridad de la información para el colegio Germán Arciniegas se llevarán a cabo la planeación y el control operacional, se evaluará el desempeño del SGSI mediante la planeación y ejecución de las auditorías internas y de acuerdo con los resultados de las no conformidades, se procederá a realizar las mejoras a las que haya lugar, previa aprobación de las autoridades competentes.

BIBLIOGRAFÍA

ALEMÁN NOVOA, Helena y RODRÍGUEZ BARRERA, Claudia. Metodologías Para el Análisis de Riesgos en los SGSI. [En línea]. 2015. Vol. 9. Disponible en http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

ANA Arbeláez. Enter.co. [en línea]. 19 datos que usted no sabía sobre internet en Colombia. Colombia. (16 de mayo de 2014). Disponible en http://www.enter.co/cultura-digital/colombia-digital/19-datos-que-usted-no-sabia-sobre-internet-en-colombia/.

CANO MARTÍNEZ, Jeimy José. Computación Forense: descubriendo los rastros informáticos. 2 ed. Bogotá: Alfaomega Colombiana S.A. 2015. 271 p. ISBN 978-958-682-922-9.

CENTRO CIBERNÉTICO POLICÍA NACIONAL. Informe Amenazas del Cibercrimen en Colombia 2016 – 2017 [En línea]. Bogotá. 2017. Disponible en https://caivirtual.policia.gov.co/contenido/informe-amenazas-del-cibercrimen-en-colombia-2016-2017.

Cifras SIEDCO - Plataforma Estadística se Criminalidad y Operatividad de la Policía Nacional. A fecha 10/03/2017.

COLOMBIA. CONCEJO DE BOGOTÁ D.C. Acuerdo 257. (30, noviembre, 2006). Por el cual se dictan normas básicas sobre la estructura, organización y funcionamiento de los organismos y de las entidades de Bogotá Distrito Capital, y se expiden otras disposiciones. Registro Distrital 3662. Bogotá D.C. El Consejo. 2006. 31 p. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=22307

COLOMBIA. CONGRESO DE COLOMBIA. Ley 734. (05, 02, 2002). Por la cual se expide el código único disciplinario. 147 p.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 115. (8, febrero, 1994). Por la cual se expide la ley general de educación. Bogotá D.C.: El Ministerio. 1994. 50 p.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1712. (6, marzo, 2014). Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones. Bogotá D.C. El Congreso. 2014. 14 p. Disponible en: http://www.mintic.gov.co/portal/604/articles-7147_documento.pdf

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 594. (14, julio, 2000). Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones. Bogotá D.C.: El Ministerio. 2000. 15 p.

COLOMBIA. EL CONCEJO DE BOGOTÁ, D. C. Acuerdo 257. (30, noviembre, 2006). Por el cual se dictan normas básicas sobre la estructura, organización y funcionamiento de los organismos y de las entidades de Bogotá, Distrito Capital, y se expiden otras disposiciones. Bogotá D.C.: El Consejo. 2006. 31 p.

COLOMBIA. EL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Decreto 1078. (26, mayo, 2015). Por medio del cual se expide el Decreto Único reglamentario del sector de tecnologías de la información y las comunicaciones. Bogotá D.C.: El Presidente. 2015. 172 p.

COLOMBIA. EL PRESIDENTE DE LA REPÚBLICA. Decreto 1080. (26, mayo, 2015). Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura. Bogotá D.C. La Ministra de Cultura. 2015. [en línea]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=62515

COLOMBIA. LA SECRETARÍA DE DUCACIÓN DEL DISTRITO. Resolución 1944. (26, diciembre, 2016). Por medio de la cual se adopta la Política de Seguridad de la Información de la Secretaría de Educación del Distrito. Registro Distrital 5982. Bogotá. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=68201

COLOMBIA. LA SECRETARÍA DE EDUCACIÓN DEL DISTRITO. Resolución 599. (28, marzo, 2014). Por medio de la cual se conforma el Comité Interno de Archivo de la Secretaria de Educación del Distrito, se reglamenta su funcionamiento y se deroga la Resolución 856 del 25 de abril de 2012. Bogotá D.C. 2014. [En línea]. Disponible http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=60457

COLOMBIA. LA SECRETARÍA DE EDUCACIÓN DEL DISTRITO. Resolución No. 161. (24, enero, 2008). Por la cual se separa del Colegio Basilia la sede de ampliación Brasil López Quintana, tomando el nombre de Colegio Germán Arciniegas.

COLOMBIA. LA SECRETARÍA DE EDUCACIÓN DEL DISTRITO. Resolución No. 1525. (1, septiembre, 2017). Por la cual se establece el proceso de gestión de la cobertura 2017 — 2018, en el Sistema Educativo Oficial de Bogotá. La Secretaría. 26p.

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. Documento CONPES: lineamientos de política para ciberseguridad y ciberdefensa. Bogotá D.C.: La Institución, 2011. 43 p.

DIARIO EL AMANECER. Herramientas educativas para generar recursos digitales. [En línea]. Historia de Internet en el mundo y su llegada a Colombia. Colombia. (Marzo de 2015). Disponible en http://es.calameo.com/read/0042539398be5661ee9aa.

EL PORTAL DE ISO 27001 EN ESPAÑOL. [En línea]. [Consultado 12 de marzo de 2018]. Disponible en http://www.iso27000.es/.

EL TIEMPO. A diario se registran 542.465 ataques informáticos en Colombia. [En línea] Bogotá D.C. 2017. Disponible en: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/informe-sobre-ataques-informaticos-en-colombia-y-al-sector-financiero-135370.

EL TIEMPO. Archivo. [En línea]. Así fue la primera comunicación telegráfica. Colombia. (1 de noviembre de 1995). Disponible en http://www.eltiempo.com/archivo/documento/MAM-442432

FUNDACION CARLO JLIM. Vulnerabilidades informáticas. [En línea]. Disponible en: https://capacitateparaelempleo.org/assets/4aq4l6q.pdf

GUZMÁN LUCERO, Álvaro Fernando. Programa de gestión documental Secretaría de Educación del Distrito. [En línea]. Bogotá: Secretaría de Educación del Distrito. 2017., 41 p. Disponible en: https://www.educacionbogota.edu.co/archivos/Nuestra_Entidad/Gestion/Gestion%20Documental/2018/Programa_gestion_documental_2017.pdf

INFORME AMENAZAS DEL CIBERCRIMEN EN COLOMBIA 2016 – 2017 [En línea]. Bogotá: Centro cibernético Policía nacional. 2017. Disponible en https://caivirtual.policia.gov.co/contenido/informe-amenazas-del-cibercrimen-en-colombia-2016-2017.

INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Código de práctica para controles de seguridad de la información: técnicas de seguridad. NTC-ISO/IEC 27002. Bogotá D.C.: El Instituto, 2015. 110 p.

INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Gestión de Incidentes de seguridad de la información: técnicas de seguridad. GTC-ISO/IEC 27035. Bogotá D.C.: El Instituto, 2012. 91 p.

INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Gestión del riesgo en la seguridad de la información: técnicas de seguridad. NTC-ISO/IEC 27005. Bogotá D.C.: El Instituto, 2009. 63 p.

INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Sistemas de gestión de la seguridad de la Información: técnicas de seguridad y requisitos. NTC-ISO/IEC 27001. Bogotá D.C.: El Instituto, 2013. 26 p.

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. G.INF.07 Guía para la gestión de documentos y expedientes electrónicos, Guía Técnica, versión 1.0, 14 de noviembre de 2017.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Columnas Ministro TIC. [En línea] Bogotá D.C. 2017. Disponible en: http://www.mintic.gov.co/portal/604/w3-propertyvalue-14674.html.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Estudio sobre el impacto económico de los incidentes, amenazas y ataques cibernéticos en Colombia. [En línea] Bogotá D.C. 2017. Disponible en: http://micrositios.mintic.gov.co/ciberestudio/.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Gobierno en línea. Glosario. {En línea}, {3 de marzo de 2018}. Disponible en: http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7742.html.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Gobierno de Colombia. [En línea]. Historia. Colombia. (26 de febrero de 2018). Disponible en http://www.mintic.gov.co/portal/604/w3-propertyvalue-6077.html.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA), EL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA (MINTIC) Y EL BANCO INTERAMERICANO DE DESARROLLO (BID). Informe Impacto de los incidentes de seguridad digital en Colombia 2017. [En línea]. 2017. Disponible en https://publications.iadb.org/handle/11319/8552?locale-attribute=es&.

COLEGIO GERMÁN ARCINIEGAS. Pacto de convivencia. [En línea]. Bogotá: Colegio Germán Arciniegas. 2018., 166 p. Disponible en: http://www.colegiogermanarciniegas.edu.co/institucional/PACTO-DE-CONVIVENCIA.pdf

PORTAFOLIO. FINANZAS. [En línea]. IBM Colombia siete décadas de innovación. Colombia. (30 de octubre de 2007). Disponible en http://www.portafolio.co/economia/finanzas/ibm-colombia-siete-decadas-

innovacion-llegada-compania-ofrecio-pais-relojes-balanzas-maquinas-escribir-tabulacion-386158.

EL TIEMPO, del 27 de septiembre de 2017 en http://www.eltiempo.com/tecnosfera/novedades-tecnologia

SECRETARÍA DE EDUCACIÓN DEL DISTRITO. Directorio único de establecimientos educativos de Bogotá. [En línea]. (2018). Disponible https://dueb.educacionbogota.edu.co/Dueb/colegioListado.sed.

SEMANA. TENDENCIAS. [En línea]. La máquina que cambió al país. Colombia. (30 de octubre de 2007). Disponible en https://www.semana.com/especiales/articulo/marzo-1957-brla-maquina-cambio-pais/65917-3.
%