DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI BASADO EN LA NORMA ISO27001 PARA EL COLEGIO PRO-COLOMBIANO DE LA CIUDAD DE BOGOTÁ, QUE INCLUYE: ASESORIA, PLANEACIÓN

JERZON HERLEY ALVAREZ RIAÑO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2016

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI BASADO EN LA NORMA ISO27001 PARA EL COLEGIO PRO-COLOMBIANO DE LA CIUDAD DE BOGOTÁ, QUE INCLUYE: ASESORÍA, PLANEACIÓN

JERZON HERLEY ALVAREZ RIAÑO

Proyecto de grado del área del Conocimiento - Gestión de la Seguridad Informática: Área Específica: SGSI basado en ISO27000 e ISO27001

Director
Ing. MARTIN CAMILO CANCELADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2016

CONTENIDO

PAG

LISTA DE TABLAS

PAG

LISTA DE FIGURAS

PAG

LISTA DE ANEXOS

PAG

INTRODUCCIÓN

Teniendo en cuenta que la información es uno de los activos más importantes de las organizaciones, se han definido normas y regulaciones basadas en estándares internacionales (ISO27000 e ISO27001) que buscan regular el adecuado manejo, custodia y protección de la información entregada por las personas naturales y jurídicas; estas regulaciones tienen como objetivo proteger el derecho a la privacidad y confidencialidad de la información y garantizar que ésta tenga el uso requerido según el objeto social de la empresa.

Con los adelantos tecnológicos la información en medios físicos disminuyó sustancialmente dando paso al formato digital, generando beneficios a las instituciones, ya que facilitó su manejo y consulta, disminuyó los costos generados en la utilización de espacios amplios para su almacenamiento y la protegió del deterioro causado por el paso del tiempo y una inadecuada conservación.

No obstante lo anterior, así como trajo beneficios también se convirtió en un foco de atención y apetito para delincuentes informáticos que por las debilidades que detectaron en los sistemas de información se les facilitó apropiarse indebidamente de la misma, ya sea para tener el poder económico que da la información o para fines delictivos.

Por lo anterior, es fundamental que la entidades se concienticen de la importancia de contar con un adecuado sistema de gestión de seguridad de la información que administre los riesgos a los que están expuestos los activos de información de la empresa y de sus clientes, identificando las amenazas y vulnerabilidades y mitigando su materialización a través de controles efectivos y eficientes que garanticen razonablemente la protección de la información, tanto de factores internos como externos.

1. PLANTEAMIENTO DEL PROBLEMA

1.1. DEFINICIÓN DEL PROBLEMA

Realizada visita a la institución colegio PRO-COLOMBIANO y de acuerdo a información suministrada por parte de los directivos de la institución, se detectó que en la actualidad la institución no cuenta con un sistema de gestión de seguridad de la información implementado, lo que hace que la información que se manipula este en alto riesgo ya que al no contar con el SGSI se concluye que no hay políticas de seguridad establecidas para la protección de la información, el personal no es consciente de la importancia de la protección de la información confidencial esto hace que no exista control sobre la información haciéndola vulnerable y no existiendo conciencia del autocontrol y vigilancia de este activo.

El contexto de funcionamiento del colegio hace que se manipule a diario información confidencial, llámese datos personales de los alumnos, padres de familia, personal docente entre otros, adicionales a las calificaciones de los alumnos que estudian en esta institución.

Como se expresó en el párrafo anterior, la información tanto de los padres y alumnos, lo que incluye si estos están o no afiliados al SISBEN, estrato socio económico, dirección de residencia, números de contacto entre otras debe ser suministrada al ministerio de educación mediante el “SIMAT” Sistema de Matrícula Estudiantil de Educación Básica y Media, adicional a que a fin de año se deben reportar los alumnos que aprobaron o no el año lectivo, para lo cual la institución tiene asignado un usuario y claves únicas y exclusivas.

El Ministerio de educación Mediante el SIMAT facilita la inscripción de alumnos nuevos, el registro y la actualización de los datos existentes del estudiante, la consulta del alumno por Institución y el traslado a otra Institución, entre otros. Se logra sistematizar, consolidar y analizar la información. De esta manera, se mejoran los procesos de inscripción, asignación de cupos y matrícula, y por ende el servicio a la comunidad.

De acuerdo al decreto 1290, cada institución educativa del sector privado define los métodos de evaluación y promoción de los alumnos generando y asignando las calificaciones que cada estudiante obtiene para definir si aprueba o no las asignaturas cursadas en la institución, el colegio solo debe reportar a fin de año lectivo cuales alumnos aprobaron o no el año y están habilitados para ingresar al grado siguiente.

1.2. FORMULACIÓN DEL PROBLEMA

¿Cómo el diseño de un SGSI basado en la norma ISO/IEC 27001 ayudará a minimizar las vulnerabilidades y amenazas de seguridad de la información que se presentan en el colegio PRO-COLOMBIANO de la ciudad de Bogotá?

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Minimizar las vulnerabilidades y amenazas de seguridad de la información con el diseño de un SGSI para el colegio PRO-COLOMBIANO de la ciudad de Bogotá

2.2. OBJETIVOS ESPECÍFICOS

- ✓ Establecer los activos de información, de infraestructura tecnológica, sistemas de información e información que existen en el colegio PRO-COLOMBIANO con el propósito de definir los alcances del SGSI
- ✓ Programar un plan de pruebas a llevar a cabo en el Colegio PRO-COLOMBIANO, para así determinar el nivel de seguridad en que se encuentra la institución.
- ✓ Identificar las vulnerabilidades amenazas y riesgos existentes en la seguridad de la información, con el propósito de valorar la probabilidad y el impacto en el evento de que se materialicen riesgos de seguridad de la información en lo concerniente a la confidencialidad, integridad y disponibilidad de la información.
- ✓ Diseñar un manual del SGSI de acuerdo a los resultados anteriores que contenga las políticas, normas y procedimientos de seguridad de la información e implementación de controles en el Colegio PRO-COLOMBIANO.

3. JUSTIFICACIÓN DEL PROYECTO

En este mundo donde todo gira en torno al manejo, aprovechamiento y utilización de la información es fundamental que esta esté siempre resguardada ante posibles amenazas y atacantes que puedan utilizarla con propósitos delincuenciales, ya sea para beneficio propio, redención económica o solo por causar daños a la institución y afectar su buen nombre.

Es innegable la importancia de la protección de la información en cualquier organización sea cual sea su razón de ser la cual representa su activo más valioso, en este caso la información personal tanto de padres como alumnos así como de las calificaciones de los alumnos, información del personal administrativo y docente así como de los activos de la institución educativa colegio PRO-COLOMBIANO.

Con el desarrollo de este proyecto, la institución educativa colegio PRO-COLOMBIANO y en especial sus dueños y directivas, podrán identificar los activos de información con los cuales cuenta ya que a la fecha no poseen un inventario actualizado de estos, conocerán las amenazas y vulnerabilidades y los posibles riesgos a los que se pueden enfrentar y que pueden afectarlos, establecer procedimientos y controles que permitan una rápida detección y respuesta ante incidentes de seguridad.

Clientes llámese padres de familia, alumnos y los funcionarios que laboran en esta institución tendrán la tranquilidad y seguridad de pertenecer a una institución en la cual se garantiza el buen manejo de la información ya que con el desarrollo de este proyecto se definirán políticas tendientes al buen manejo de los activos de información que incluyen sus datos personales.

La institución al contar con un sistema de gestión de seguridad de la información garantiza la buena gestión de los riesgos según estándares internacionales, minimizándolos lo que hará que tenga la posibilidad de certificarse haciendo que su nombre sea más valorado atrayendo nuevos alumnos y manteniendo los existentes.

Adicionalmente los resultados operacionales mejoraran al contar con políticas y procedimientos estandarizados para todos los procesos que tengan que ver con el manejo y la manipulación de la información los gastos operacionales se reducirán y la institución garantiza la integridad de la información y con ello la continuidad del negocio.

4. ALCANCE Y DELIMITACIÓN DEL PROYECTO

Siendo conscientes que un alcance excesivo puede causar que el proceso sea inabordable y cause su fracaso ya sea por razones de tiempo o por consumo excesivo de recursos, se acordó con las directivas de la institución delimitar el proyecto a ciertos procesos llevados a cabo en el funcionamiento interno del colegio.

El alcance definido para la implementación del sistema de gestión de seguridad de la información en la institución educativa colegio PRO-COLOMBIANO está enfocado a los procesos de matrícula y procesamiento de las calificaciones de los alumnos de la institución.

5. MARCO REFERENCIAL

5.1. ANTECEDENTES

Debemos iniciar el enfoque de este proyecto, partiendo de los requerimientos identificados y que ponen en riesgo los activos de información de los procesos de matrículas y gestión de calificaciones del colegio PRO-COLOMBIANO de la ciudad de Bogotá, para los cuales se plantea la realización del análisis de riesgos basados en la revisión de algunos antecedentes previos.

En la actualidad la norma ISO 27001 es fundamental para toda empresa que quiera demostrar fortaleza en la gestión de la seguridad de la información, y en Colombia debe ser de obligatorio cumplimiento para todas aquellas empresas u organizaciones que sean consideradas como operadores de información, debido a lo fundamental que es la implementación de un SGSI para la gestión de riesgos que propendan para la protección de la información y para tener un buen gobierno corporativo.

Así como lo expresa la norma aplicada en Colombia *"Para funcionar eficazmente, una organización debe identificar y gestionar muchas actividades. Se puede considerar como un proceso cualquier actividad que use recursos y cuya gestión permita la transformación de entradas en salidas. Con frecuencia, el resultado de un proceso constituye directamente la entrada del proceso siguiente"*[1], se denota la importancia que tiene la gestión en los procesos llevados a cabo en las organizaciones, en este caso particular en el colegio PRO-COLOMBIANO.

Por esto y de acuerdo a la norma NTC-ISO/IEC 27001 que indica "*La organización debe establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI documentado, en el contexto de las actividades globales del negocio de la organización y de los riesgos que enfrenta",* y a los antecedentes que se tienen en otras organizaciones, se reafirma la necesidad de la implementación de un sistema de gestión de seguridad de la información en cualquier ámbito empresarial.

Las empresas que se han certificado con ISO 27001 son aquellas donde la información y el manejo de la misma son el activo más importante para su funcionamiento, es más, podemos decir que la información crítica en una organización no solo es la que está presente en medios magnéticos, también es considerada como información crítica aquella contenida en papel, archivada en

[1]NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001

diferentes medios, la que es transmitida a terceros, se comparte en conversaciones y la presente en el conocimiento de las personas.

Para dar una alerta y asimismo poner en evidencia la importancia del tema a desarrollar en el proyecto propuesto, se pone en conocimiento de las directivas de la institución un caso relevante sucedido en Colombia específicamente en la Universidad Mariana de la ciudad de Pasto en el cual se presentó fraude en el sistema de almacenamiento de resultados de evaluaciones y asistencia de los alumnos.

Es así que para contextualizar la importancia del tema y se denote la premura de la implementación de un Sistema de gestión de seguridad de la Información (SGSI) en la institución Colegio PRO-COLOMBIANO objetivo de este proyecto, se cita textualmente parte del informe del caso mencionado en el párrafo anterior “Los primeros indicios señalan que la red de computadores que cumple la tarea de recibir y archivar los resultados de las evaluaciones y los registros de asistencia a clase de los estudiantes, habrían sido "hackeados" por personas interesadas en establecer una especie de "mercado de notas", como lo indicó el padre de una alumno de la entidad, quien además de pedir la reserva de su nombre, señaló que le llegaron a pedir hasta 2 millones de pesos por alterar la nota de una evaluación parcial.”[2]

Aunque el tema de la protección de los activos de información y de los activos informáticos ha tomado mucha relevancia en Colombia, es poca la teoría disponible en el tema de implementación de Sistemas de gestión de seguridad de la información aplicada a instituciones educativas en Colombia.

Para el desarrollo de esta propuesta, podemos mencionar como antecedentes en el ámbito nacional, el trabajo de investigación denominado “IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN LA COMUNIDAD NUESTRA SEÑORA DE GRACIA, ALINEADO TECNOLÓGICAMENTE CON LA NORMA ISO 27001” presentado por los estudiantes Andrés Fabián Díaz, Gloria Isabel Collazos, Hermes Cortez Lozano, Leidy Johanna Ortiz, Gustavo Adolfo Herazo Pérez estudiantes de Ingeniería de sistemas de la Universidad Konrad Lorenz de la ciudad de Bogotá con el fin de implementar un SGSI en la Comunidad Nuestra Señora de Gracia en el cual establecieron políticas y controles de mejoramiento de los procesos de seguridad de la información y se definieron las declaraciones de aplicabilidad que fortalecieron todo el análisis de riesgos efectuado.

[2]Tonado de Página10, articulo Fiscalía investiga posible fraude de notas en la Universidad Mariana, disponible en: http://pagina10.com/index.php/judicial/item/6375-fiscalia-investiga-posible-fraude-de-notas-en-la-universidad-mariana#.V-A4wPl97IU

Con la teoría expuesta en dicha investigación, se puede evidenciar que en las instituciones educativas dígase en este caso particular colegios, el tema de la seguridad de la información y de los procesos tendientes a la protección de los activos de información no tiene la relevancia que amerita, ya sea por desconocimiento de las normas que actualmente aplican, o simplemente por decisiones administrativas.

Se tiene también como antecedente el artículo denominado “Desarrollo de un SGSI para los colegios Profesionales en la Región de Lambayeque, Caso de estudio: Colegio de Ingenieros” publicado en la revista de la Universidad católica santo Toribio de Mogrovejo de la ciudad de Chiclayo – Perú por los ingenieros Cesar Augusto Córdova Oblitas, Gustavo Alfredo Morales Cueva y José Antonio Samamé Martínez.

En el mencionado artículo se denota la problemática existente debido a la falta de seguridad de la información (SI) en dicha organización debido a la falta de controles lo que dificulta el cumplimiento de los objetivos estratégicos y el cómo las organizaciones educativas para este caso particular solo reaccionan de forma reactiva ante eventos que afecten la seguridad de la información y el como la implementación de un SGSI ayudad a reaccionar de manera proactiva ante dichos eventos.

Adicionalmente los autores tienen como objetivo culturizar a la alta dirección sobre la seguridad de la información, analizar las brechas, la identificación de riesgos, identificación y evaluación de controles, plantear proyectos de seguridad de la información y el uso de la norma ISO 27001 para el desarrollo de la investigación.

Este artículo sirve como referencia para evidenciar a los directivos en la institución educativa Colegio PRO-COLOMBIANO el problema latente y sirve como base fundamental para la argumentación de conceptos a aplicar en el desarrollo de este proyecto al evidenciarse situaciones similares presentes en la institución colegio PRO-COLOMBIANO.

Como otros antecedentes y para el caso de instituciones educativas a nivel mundial, se pueden nombrar el Warnborough College en el reino Unido y La Universidad del Estado de Georgia quienes al tener acreditados sus procesos después de haber implementado sistemas de gestión de seguridad de la información han tenido acceso a las auditorías de terceros, creando una visión de conjunto de credibilidad y la transparencia, logrando niveles de seguridad más altos para mantener seguros

los datos de los estudiantes y del cuerpo docente e invocando la mejora continua en la obtención y gestión de información.

De acuerdo a estos antecedentes analizados y presentados a las directivas de la institución educativa colegio PRO-COLOMBIANO adicional a la situación presente en la institución la cual de acuerdo a un estudio previo realizado para poder presentar la propuesta objeto de este proyecto, la institución presenta falencias en los procesos relacionados para el aseguramiento manejo y custodia de información confidencial, situación que se puso su conocimiento respecto a las amenazas y riesgos que se enfrentan el tema de la protección de sus activos de información y la importancia que tiene la implementación de un sistema de gestión de seguridad de la información en su institución para la minimización de los riesgos, razón por la cual se les hizo la propuesta para su implementación en sus procesos la cual esta descrita en este documento y que fue avalada por ellos.

5.2. MARCO CONTEXTUAL

La propuesta objeto de este proyecto se realizará en el colegio PRO-COLOMBIANO de la ciudad de Bogotá.

5.2.1. Reseña histórica.

El colegio fue fundado en el año de 1.977 por iniciativa de la Señora María Elisa de Campuzano, en el barrio Meissen, al sur de la ciudad, ella quien siempre manifestó el deseo de brindar educación a los niños y niñas de bajos recursos económicos de la zona, por quebrantos de salud y debido a su avanzada edad decide dejar su labor en manos de ROSA EDELMIRA SALAZAR SALAMANCA, quien normalista, licenciada en básica primaria y con estudios de economía podría continuar con su labor con la misma filosofía que dieron origen a la institución educativa.

El colegio inicia una nueva etapa en 1.992, año en que es trasladado al barrio San Carlos, para continuar con la labor educativa en una mejor planta física con buenas condiciones y en un sector que no contaba con una centro educativo con la filosofía de PRO-COLOMBIANO.

El primero de noviembre de 1993 recibe la visita de supervisor de la zona 6°.Para aprobar la nueva Sede y la aprobación de cursos con la satisfacción del señor supervisor quien deja una serie de inquietudes para corregir. Se aplicaron los correctivos correspondientes a las observaciones del funcionario y en diciembre de

1994 obtiene el número de aprobación 5964 de la secretaria de educación de Bogotá para su nueva sede.

La institución no ha perdido su identificación con el sector pobre de la ciudad. Está creando un ambiente educativo de formación integral, que facilite la participación, expresión y superación, se han fortalecido las actividades recreativas, deportivas, artísticas con el fin de aprovechar el tiempo de formación y elevar la autoestima.

Sus valores son la base de su afianzamiento en el sector en la enseñanza básica primaria, generando confianza en los padres de familia quienes depositan la confianza de la educación de sus hijos en la institución al considerarla que trabaja con grandes estándares de calidad.

5.2.2. Misión. Integrar y formar la comunidad Educativa con el propósito de:

- Orientar a los estudiantes en el desarrollo armónico de su personalidad y en la construcción de su proyecto de vida centrado en los valores.
- Potenciar espíritu crítico e investigativo con criterios de calidad para solucionar problemas en la cotidianidad.
- Crear un ambiente educativo rico en valores y respeto de los derechos humanos.
- Proyectar a la comunidad la acción educativa y las experiencias.

5.2.3. Visión. La comunidad educativa busca formar:

- Niños y niñas sensibles ante los problemas de la sociedad y dispuestos a colaborar en la solución.
- Niños y niñas con alta calidad humana rica en valores: tolerancia, respeto, justicia, benevolencia, verdad.
- Niños y niñas capaces de crear, innovar, desempeñarse en grupo con calidad y sentido social
- Jóvenes conocedores y respetuosos de los Derechos Humanos.

5.2.4. Organigrama institucional.

El organigrama y el manual de funciones presentan por un lado las relaciones que se establecen entre los diferentes estamentos y por el otro las funciones y responsabilidades que les corresponde ejercer a cada uno de los miembros para distribuir la tarea educativa y administrativa del establecimiento, con el fin de

avanzar en el camino hacia la consecución de las metas y objetivos propuestos en el PEI.

Las funciones bien definidas y ejercidas con responsabilidad y sentido de pertenencia, promueve la participación y generan un clima de organización, armonía y orden la de la institución.

Figura 1. Organigrama institucional colegio PRO-COLOMBIANO

Fuente: Colegio PRO-COLOMBIANO

5.2.5. Descripción de procesos y procedimientos de matrícula y calificaciones.

Es fundamental que se conozcan los procesos llevados a cabo en la institución y en especial los procesos definidos dentro del alcance definido de este proyecto, que son matrículas y calificaciones, para así poder identificar las debilidades que se presenten y que puedan llevar a la materialización de amenazas aprovechando las vulnerabilidades y que puedan generar riesgos a los activos de información inherentes a dichos procesos, estos se describen a continuación.

5.2.6. Proceso de matrículas.

El proceso de matrículas en el colegio PRO-COLOMBIANO implica que los padres o acudientes obtengan y diligencien el formulario de inscripción obligatorio para todo estudiante nuevo o antiguo en la institución (ver Anexo C), diligenciándolo completamente el cual es estudiado por las directivas de la institución quienes definen si el aspirante puede ser aceptado o no como alumno de la institución.

Teniendo el aval por parte de las directivas de la institución, se informa al padre o acudiente que el estudiante es admitido en la institución y que debe presentarse en las fechas establecidas para formalizar su matrícula adjuntando los documentos solicitados por la institución.

Entre los documentos requeridos se tienen:

- Registro Civil.
- Fotos recientes (color, 3x4).
- Paz y Salvo por concepto de pensiones y servicios, expedido por el colegio o jardín infantil, correspondiente al año anterior.
- Informe del colegio anterior: Comportamiento.
- Notas de todos los grados cursados hasta el presente año.

Para todo alumno aceptado y matriculado en la institución, se crea una hoja de matrícula (ver Anexo D) la cual se adjunta al libro de matrículas consignándola en el archivo de la institución junto con los documentos del estudiante y datos de los padres y/o acudientes.

Al finalizar el proceso de matrículas, la institución debe reportar ante el Ministerio de Educación Nacional los datos de los alumnos matriculados en la institución, proceso que la institución realiza utilizando la herramienta en línea SIMAT (Sistema integrado de matrículas) disponible en el siguiente link: http://www.sistemamatriculas.gov.co/simat/app, para lo cual el Ministerio de educación asigna a cada institución un usuario y claves únicas.

En la Figura 2 (Proceso de matrículas colegio PRO-COLOMBIANO), se contextualiza el proceso llevado a cabo en la institución para el proceso de matrículas de sus estudiantes.

Figura 2. Proceso de matrículas colegio PRO-COLOMBIANO

Fuente: El autor

5.2.7. Proceso de generación de calificaciones.

El proceso de evaluación del estudiante del colegio PRO-COLOMBIANO se hace de acuerdo a los lineamientos de la Ley General de Educación y el del Decreto 230 del 11 de febrero de 2002, y busca apreciar, estimular y emitir juicios sobre los procesos de desarrollo de los estudiantes, comprobando los avances que han alcanzado en relación con los logros propuestos, y destrezas que han desarrollado, las actitudes y valores que han asumido y se han apuntalado.

De acuerdo a lo establecido en el S.I.E del colegio PRO-COLOMBIANO en el "**ARTICULO 13. PERIOCIDAD DE ENTREGA DE INFORMES ACADÉMICOS A LOS PADRES DE FAMILIA,** se determina que:

Se entregaran informes académicos a los padres de familia cada 2 meses en forma bimensual para un total de 4 entregas al año y se dejara un registro final el cual se utilizará para la expedición de certificados; este último registro será el promedio del estudiante durante los cuatro periodos anteriores.[3]

La estructura del informe escrito manifestara el rendimiento académico de cada estudiante al igual que sus falencias y observaciones obtenidas al final del año

[3] S.I.E. (Sistema integrado de evaluación) colegio PRO-COLOMBIANO

escolar teniendo como referente la escala numérica y su asimilación a la escala nacional expedida por el MEN (Ministerio de educación Nacional.
La evaluación es un proceso continuo e integral y se hace con referencia a cuatro periodos de igual duración en los que se dividirá el año escolar. Los principales objetivos de la evaluación son:

1. Valorar el alcance y la obtención de logros, competencias y conocimientos por parte de los educandos.
2. Determinar la promoción o no de los educandos en cada grado de la educación básica y media.
3. Diseñar e implementar estrategias para apoyar educandos que tengan dificultades en sus estudios.
4. Suministrar información que contribuya a la autoevaluación académica y a la actualización permanente de su plan de estudios.

De este proceso se generan varios documentos entre los cuales se menciona y describen a continuación:
Informe académico periódico: boletín informativo que contiene las calificaciones asignadas al estudiante en cada periodo académico y que se entrega mensualmente a los padres, el cual pueden conservar. (Anexo D)

Observador del estudiante: en este reporte se consignan los datos de los acudientes adicionales a los del alumno, informándole de las apreciaciones y avances del estudiante, este reporte debe ser valorado por el padre o acudiente firmarlo y devolverlo a la institución.

Sabana de notas: documento que cada profesor de la institución debe diligenciar incluyendo el consolidado de todas las notas de los estudiantes a lo largo de los periodos académicos. (Anexo E)

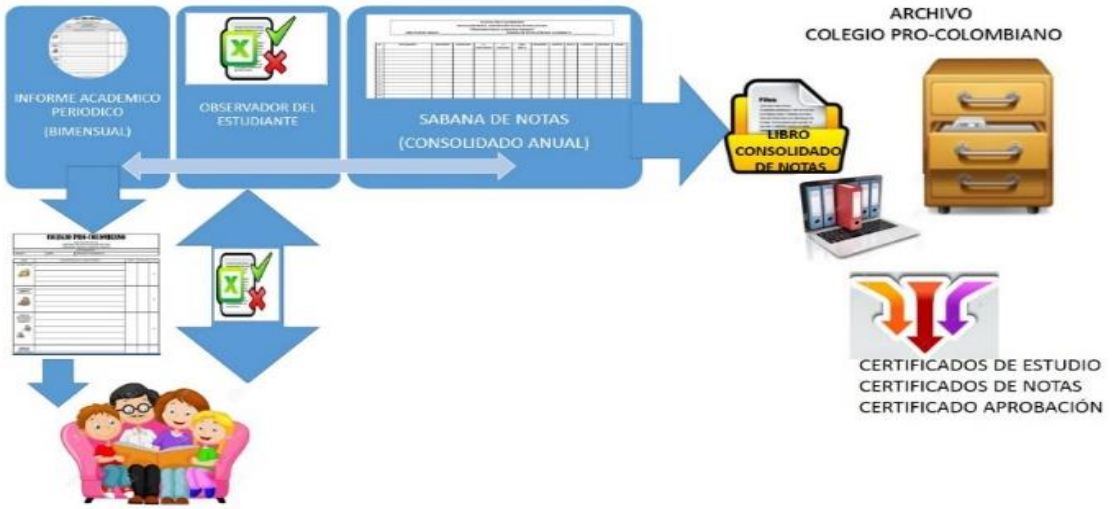
PARAGRAFO: De acuerdo a lo establecido en el S.I.E (Sistema integrado de evaluación) definido por las directivas del colegio PRO-COLOMBIANO, el cual cita textualmente: *"Cada docente llevará un registro de valoración integral de estas cuatro dimensiones del estudiante en su área respectiva, más la autoevaluación y el resultado de esta será la valoración final de área. El Consejo Académico establecerá el formato o formatos necesarios para el registro de las valoraciones de aprendizaje de los estudiantes teniendo en cuenta los criterios consignados en el presente acuerdo."*[4]

Toda la documentación propia del proceso de calificaciones es archivada en el libro consolidado de notas y resguardado en el archivo de la institución.

[4] S.I.E. (Sistema integrado de evaluación) colegio PRO-COLOMBIANO

En la Figura 3 se presenta un gráfico que ambienta los procesos antes descritos.

Figura 3. Proceso calificaciones colegio PRO-COLOMBIANO



Fuente: El autor

5.2.8. Archivo de la institución.

Como se ha descrito previamente en la descripción de los procesos de matrículas y calificaciones llevados a cabo en la institución, en los cuales se genera información adicional a la documentación recibida de sus alumnos y acudientes sumada a la información propia del funcionamiento información que debe considerarse de carácter confidencial y que por su importancia debe ser resguardada evitando su perdida, robo o destrucción, lo cual se realiza en el archivo general de la institución.

El archivo de la institución es el principal insumo y fuente para la generación de certificados de notas y de estudio requeridos tanto por alumnos como por ex alumnos de la institución, información requerida para traslado del estudiante a otras instituciones, solicitud de auxilios, entre otras, así como los funcionarios de la institución.

Cabe recordar que toda esta información consignada en el archivo, referente a notas y datos de matrículas de los alumnos debe estar reportada ante el Ministerio de educación, razón por la cual es fundamental su buen resguardo, pues en caso de reclamaciones por parte de estos entes esta información es el insumo con el que cuentan, además para la toma de decisiones institucionales y de inversión así como certificar la aprobación o no de un curso por parte de un estudiante.

La Figura 4 ilustra la disposición del archivo de la institución.

Figura 4. Archivo colegio PRO-COLOMBIANO

Fuente: El autor

5.3. MARCO TEÓRICO

Las normas, políticas y procedimientos establecidos para el tratamiento de la información que buscan su protección están encaminados a preservar este activo de vital importancia para el funcionamiento de cualquier organización, generando grandes beneficios en el desarrollo de las actividades realizadas con el fin de generar buenas prácticas empresariales y por ende generando ganancias como la agilidad en los procesos y buen nombre de la organización ante los interesados y clientes.

Herramientas organizacionales adicionales tales como capacitaciones o charlas acerca del tema generan conciencia en los empleados y directivas para la preservación de la información generada y tratada en el normal funcionamiento de las organizaciones, de su seguridad son fundamentales.

Se busca garantizar los tres principios básicos de la seguridad de la información establecidos: confidencialidad, integridad y disponibilidad, lo cual quiere decir que la información no sea ofrecida a personas o entidades externas y no autorizadas con lo cual se garantiza la confidencialidad, garantizando que solo personas

autorizadas y bajo control tengan salvoconducto para realizar modificaciones hablando así del principio de Integridad, y que la información este siempre disponible a las personas autorizadas hablando así de la disponibilidad.

También la utilización de estándares como la familia ISO27000, ayuda al establecimiento de metodologías de reconocimiento y control en las áreas de una organización.

Norma ISO/IEC 27000: Familia de estándares donde especifica claramente los parámetros sobre seguridad de la información, para desarrollar, implementar y mantener los sistemas de gestión de seguridad de la información, en la Tabla 1 se puede observar la descripción de estas normas, entre ellas:

Tabla 1. Familia normas ISO 27000

Norma	**Descripción**
Norma ISO/IEC 27001	Define los requisitos para la implementación de un SGSI (Sistema de Gestión de la Seguridad de la Información)
Norma ISO/IEC 27002	(Anterior ISO 17799). Es una guía de buenas prácticas, describe los controles a seguir dentro del marco de la seguridad de la información; enmarcados en 11 dominios, 39 objetivos de control y 133 controles.
Norma ISO/IEC 27003	Proporciona ayuda y orientación sobre la implementación de un SGSI, incluye el método PHVA (planear, hacer verificar y actuar) contribuyendo con revisiones y mejora continua.
Norma ISO/IEC 27004	Especificará las métricas y técnicas de medición para determinar la eficacia de un SGSI y de sus controles. Aplicable específicamente en la fase del hacer (Do); de acuerdo con el método PHVA
Norma ISO/IEC 27005	Suministra directrices para la gestión del riesgo en la seguridad de la información.

Fuente: El autor

Pero para poder establecer estas normas o políticas en pro de la protección de la información, es necesario que se realicen procesos tendientes en a la identificación

de los activos a proteger, posteriormente caracterizar las amenazas y vulnerabilidades y posibles riesgos a los que se pueden enfrentar para finalmente implementar los controles tendientes a minimizar o llevar a la mínima expresión estos, garantizando así la protección y seguridad deseada, y como una consecuencia directa de esto asegurar la continuidad del negocio .

Todo lo expuesto anteriormente es posible mediante la implementación en las organizaciones de un sistema de gestión de seguridad de la información - SGSI, para lo cual la norma NTC-ISO/IEC 27001 es una guía para la implementación de los procesos que lleven a cumplir el objetivo de proteger el activo más importante en toda organización denominado información y datos.

En concordancia con lo establecido en las recomendaciones establecidas y teniendo como base principal ISO 27001:2013 en donde indica a las organizaciones que es fundamental la identificación de los problemas internos y externos que las rodean, aquí es importante aclarar que estos requerimientos son inherentes a todo tipo de organización y su alcance.

También se establece el concepto de parte interesada como elemento primordial para la definición de los alcances del Sistema de gestión de Seguridad de la Información, en donde la norma infiere que hay que priorizar la identificación y definición formal de las necesidades de las denominadas partes interesadas con relación a la seguridad de la información y sus expectativas con relación al Sistema de gestión de Seguridad de la información.

Es así que las partes interesadas que para este caso se denomina Colegio PRO-COLOMBIANO se determinarán las políticas a seguir para la protección de la información y los objetivos a definir para el proceso de gestión de los riesgos mediante la definición y posterior implementación de un Sistema de Gestión de Seguridad de la Información.

Pero hay que recalcar que el compromiso de la Alta dirección es fundamental, mostrando compromiso y entendiendo la importancia de la implementación del Sistema de Gestión de seguridad de la Información al interior de la organización, para lo cual debe prestar apoyo al proceso al garantizar la disponibilidad de recursos tanto económicos, tecnológicos y asignado oportunamente al personal los roles y responsabilidades en busca de proteger la información todo esto en concordancia y alineados con los objetivos del negocio.

Como se ha expuesto en párrafos anteriores, se busca que mediante la implementación del sistema de gestión de seguridad de la información las partes interesadas conozcan los riesgos a los que están expuestos en cuanto al manejo y tratamiento de la información, con lo cual mediante la identificación se implementen medidas tendientes a minimizar su ocurrencia mediante controles definidos para salvaguardar su activo más valioso.

Es así que mediante la documentación de las políticas definidas para el manejo de los procesos y procedimientos, las cuales deben ser difundidas al interior de la organización en este caso particular el colegio PRO-COLOMBIANO, para el conocimiento y cumplimiento por parte de sus empleados se garantiza que se cumplan con las mejores prácticas para el resguardo de los activos de información.

Otro aspecto importante es el de concientizar a los empleados de la organización en el sentido de la protección de la información, en este aspecto es considerable la capacitación del personal que la integre.
Cabe anotar que aunque los riesgos nunca se podrán eliminar o evitar en su totalidad, si se garantiza que con la implementación del sistema de gestión de seguridad de la información la ocurrencia de estos si se puede minimizar, garantiza mejores niveles de seguridad en la protección de los activos de información y consecuencias funestas al interior de la organización garantizando la consecución de los objetivos organizacionales.

El propósito fundamental del sistema de gestión de seguridad de la información es el de garantizar que los riesgos de seguridad de la información que se identifiquen en los activos de información, sean minimizados mediante la implementación de controles tendientes a evitar las causas que los generen.

En este punto es esencial definir que es un activo de información, en el contexto, ISO lo define como *"algo a lo que una organización directamente le asigna un valor y, por lo tanto, la organización debe proteger"*[5].

La seguridad de la información debe determinar lo que se requiere sea protegido y por qué, de que debe ser protegido y como protegerlo; y está definida por tres atributos:

1. Confidencialidad: Información disponible exclusivamente a personas autorizadas.

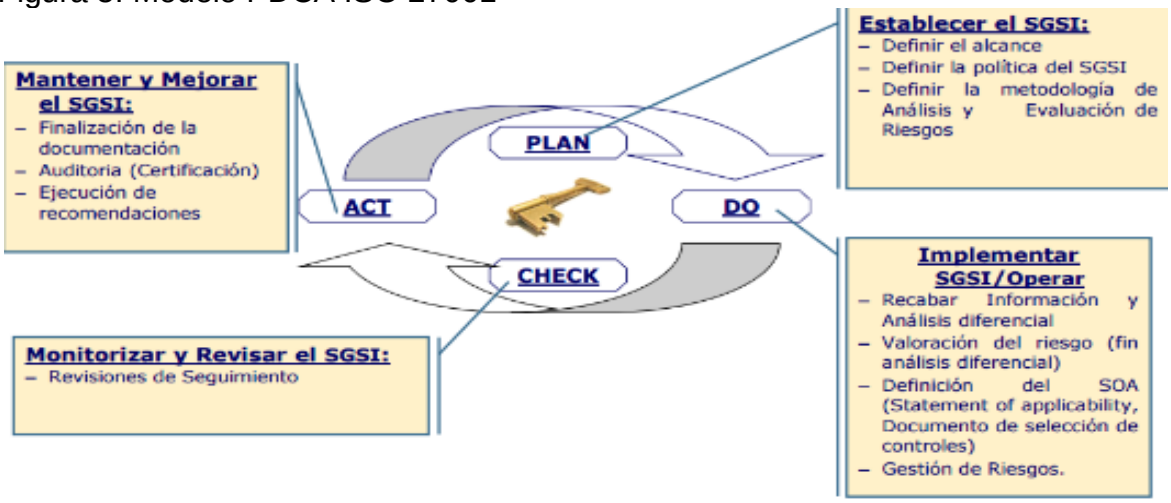
[5] Richard D. García Rondón, GESTIONAR LA INSEGURIDAD PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN: Un marco conceptual para la medición de la inseguridad, disponible en: http://52.0.140.184/typo43/fileadmin/Revista_105/RGarcia.pdf

2. Integridad: Mantenimiento de la exactitud y validez de la información, protegiéndola de modificaciones o alteraciones no autorizadas. Contra la integridad la información puede parecer manipulada, corrupta o incompleta.
3. Disponibilidad: Acceso y utilización de los servicios sólo y en el momento de ser solicitado por una persona autorizada.

Aunque garantizar niveles de prevención totales es casi que imposible, las organizaciones pueden confiar en que el sistema de gestión de seguridad de la información y mediante el seguimiento continuo de los controles establecidos se garantizan niveles óptimos para la protección de los activos de las organizaciones.

Para lograr estos objetivos se cuenta con los modelos y procedimientos establecidos como en el ciclo de Deming o PDCA determinados por ISO (International Organization for Standardization) proceso definido por 4 etapas, el cual se puede observar en la Figura 5.

Figura 5. Modelo PDCA ISO 27001



Fuente: ALARO AVANT, Protección de datos Personales y Seguridad de la Información, Implicación de la dirección. p. 26

Donde PDCA de acuerdo a su nombre en inglés significa Planificar (Plan), Implementar (Do), Medir (Check) y Mejorar (Act) y que se describe en la Figura 6.

Figura 6 Descripciones modelo PDCA

Etapa	Descripción
Planificar (Establecer el SGSI)	Establecer la política, objetivos, procesos y procedimientos del SGSI pertinentes a la gestión de riesgo y mejorar la seguridad de la información para obtener resultados de acuerdo con las políticas y objetivos generales de la organización.
Implementar (Implementar y operar el SGSI)	Implementar y operar la política, controles, procesos y procedimientos del SGSI.
Medir (Monitorear y revisar el SGSI)	Evaluar, y donde sea aplicable, medir el rendimiento del proceso contra la política del SGSI, sus objetivos y experiencia práctica, e informar los resultados para gestionar su revisión.
Mejorar (Mantener y mejorar el SGSI)	Tomar acciones correctivas y preventivas, basadas en los resultados de auditorías internas del SGSI y de revisión de gestión u otra información relevante, para lograr mejora continua del SGSI.

Fuente: RODRIGO BALDECHI, Implementación efectiva de un SGSI ISO 27001, ISACA. 2014. p.36

En la Figura 7 se puede observar la estructura definida para la implementación de un sistema de gestión de seguridad de la información.

Figura 7. Estructura de implementación de un SGSI

Fuente: ALARO AVANT, Protección de datos Personales y Seguridad de la Información, Implicación de la dirección. p. 26

Donde los documentos definidos para una correcta implementación de un SGSI son los que se describen en la Figura 8

Figura 8. Documentos del SGSI

Requisito	Descripción
Alcance del SGSI	Ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas.
Política y objetivos de seguridad	Documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.
Procedimientos y controles del SGSI	Aquellos procedimientos que regulan el propio funcionamiento del SGSI.
Declaración de aplicabilidad: (SOA -Statement of Applicability)	Documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.
Metodología de evaluación de riesgos	Descripción de la forma como se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información dentro del alcance definido, y los criterios de aceptación de riesgo.
Informe de evaluación y plan de tratamiento de riesgos	Estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización. Plan de tratamiento de los riesgos.
Plan de continuidad del negocio	Documento que identifica los planes para enfrentar diferentes escenarios. Las pruebas, los análisis del resultado de las pruebas y las acciones de mejoras del plan.
Procedimientos documentados	Todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.
Registros	Evidencia objetiva del funcionamiento del SGSI.

Fuente: RODRIGO BALDECHI, Implementación efectiva de un SGSI ISO 27001, ISACA. 2014. p.36

De acuerdo a lo anterior, la institución mediante la implementación del sistema de gestión de seguridad de la información, y conociendo las amenazas y vulnerabilidades a las que se enfrenta y mediante la implementación de controles o salvaguardas está en la posición de asumir algunos riesgos o si es el caso de transferirlos.

La institución debe tener en cuenta que el sistema de gestión de seguridad de la información que se implante, debe estar en constante revisión con el propósito de mejorar su eficacia en respuesta a los cambios internos o externos que se presenten debido a requerimientos del negocio, políticas empresariales, marco legal, entre otros lo que se lograría a través de la reforma de los controles y/o procedimientos que afecten a la seguridad de la información.

5.4. MARCO CONCEPTUAL

Para la mejor comprensión del tema a desarrollar en este proyecto, es de suma importancia dejar en claro algunos conceptos que ilustran y alertan a los interesados del porqué de la protección de la información, datos, infraestructura tecnológica, fuentes de información, los cuales son insumos fundamentales para el funcionamiento de cualquier organización.

Aceptación del riesgo: Decisión de la alta gerencia de una organización de asumir los riesgos residuales (una vez aplicados los controles) calificados en altos y extremos.

Amenaza: Son todas aquellas situaciones que pueden provocar daños a los procesos, productos y sistemas de información, que impidan el cumplimiento de los objetivos estratégicos de una organización o pérdidas de tipo económico o reputacional. No monitorear y controlar estas fallas, puede generar la materialización de los riesgos identificados en la organización.

Análisis de riesgo: Acciones que permiten identificar, medir, controlar y monitorear los riesgos inherentes y residuales mediante la mitigación de las causas y fallas que pueden ocasionar la materialización de los riesgos identificados en la organización.

Ataque: Ocurrencia o intento de vulnerar los sistemas de información para apropiación indebida o destrucción de la misma.

Control: Acción implementada para disminuir la probabilidad de ocurrencia y mitigar el impacto de los riesgos identificados.

Información: Es el conjunto de datos (digitales, físicos, orales, escritos, en imágenes, orales, impresos en papel, almacenados electrónicamente, proyectados, enviados por correo, fax o e-mail, transmitidos en conversaciones, etc.), que representan valor para el desarrollo de la función social de una organización, que han sido adquiridos a través de la ejecución de sus procesos o depositada por terceros, la cual debe ser protegida de acuerdo a su clasificación (pública o privada).

Incidente de seguridad de la información: Suceso o serie de sucesos no deseados o inesperados que pretenden vulnerar la seguridad de la información de una organización.

Confidencialidad: Calidad que se atribuye a determinada información por considerarla de acceso restringido únicamente a personal autorizado, con el fin de prevenir el uso o divulgación de la misma en forma no autorizada

Disponibilidad: La información se encuentra lista dentro de los criterios establecidos de oportunidad, calidad y conducencia para ser utilizada por todo aquel que la requiera y esté autorizado para consultarla.

Evaluación del riesgo: Metodología para identificar, medir, controlar y monitorear los riesgos, para determinar la importancia del riesgo

Seguridad: Conjunto de principios, políticas, normas, procedimientos y requerimientos definidos por una organización para salvaguardar sus activos de información.

Seguridad de la información: Directrices y lineamientos relacionados con el manejo seguro de la información, requeridas para implantar un modelo de seguridad de la información confiable y flexible para garantizar la confidencialidad, integridad y disponibilidad.

Seguridad informática: Es una declaración de deberes y de conductas a desarrollar para mantener un ambiente razonablemente seguro para **proteger la integridad, privacidad y** manejo de la información administrada en los recursos informáticos de la organización.

Sistema de gestión de la seguridad de la información SGSI: Es el conjunto de políticas necesarias para establecer, implantar, mantener y mejorar la seguridad de la Información.

Vulnerabilidades: Debilidades presentes en un sistema informático que comprometen la seguridad de la información.

Teniendo en cuenta que el enfoque de este proyecto es de la protección de los datos personales tanto de alumnos, padres de familia, docentes y del tratamiento de la información generada por las calificaciones que acrediten la aprobación de los cursos por parte de los estudiantes de la institución la cual debe ser reportada al ministerio de educación, es conveniente que los directivos y empleados de dicha institución conozcan algunos conceptos relevantes acerca de las buenas prácticas para el tratamiento y la protección de datos para evitar sanciones a los encargados y responsables del tratamiento de las bases de datos.

Estos conceptos y procedimientos se mencionan a continuación:

Datos personales: Es la información de carácter privado y confidencial que caracteriza a una persona natural, relacionada con su nombre, dirección, profesión, orientación sexual, religiosa, étnica, entre otros.

Importancia de los datos personales: Debe ser utilizada únicamente para los fines para los que fue suministrada, debido a que puede ser utilizada para fines indebidos por lo que debe ser conservada adecuadamente.

En qué consiste la protección de datos: Son las responsabilidades asociadas a la protección de los activos de información, en la que se definen responsabilidades para identificar claramente el valor de la información que administra o utiliza, conocer los riesgos a que podría estar expuesta, velar porque se provean y cumplan los mecanismos necesarios para que estos riesgos se mitiguen a niveles aceptables.

Medidas que se deben tomar para una efectiva protección de datos: Son las acciones necesarias (políticas, normas, procedimientos, principios), incluyendo aspectos disciplinarios y legales que apliquen para proteger los activos de información de la organización.

Titular de la información: Es el dueño de la información que se tiene en custodia.

Adicional a lo anterior y teniendo en cuenta lo definido en la Ley 1581 de 2012 Decreto 1377 de 2013 en el capítulo II - Procedimiento y sanciones en el artículo 23, el cual menciona:

"Sanciones: La Superintendencia de Industria y Comercio podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:

- Multas de carácter personal o institucional hasta por 2.000 Salarios Mínimos Mensuales Legales Vigentes.
- Suspensión de las actividades relacionadas con el tratamiento hasta por seis meses.
- Cierre temporal de las operaciones relacionadas con el tratamiento.
- Cierre inmediato y definitivo de la operación que involucre el tratamiento de datos."

5.5. MARCO LEGAL

En Colombia los lineamientos a seguir para la implantación de un SGSI están definidos en la norma (NTC-ISO-IEC 27001:2013) que es regularizada por el Instituto Colombiano de Normas y Técnicas y Certificación ICONTEC.

Esta norma está dirigida a ser aplicada a cualquier tipo de organización sin importar si es de carácter gubernamental, de carácter privado o sin ánimo de lucro y especifica todos los requisitos necesarios para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI que abarque todos los riesgos a los que se enfrenten las organizaciones y que se generen por el contexto del desarrollo de sus actividades.

Adicionalmente en esta norma se especifican los requisitos que requieren las organizaciones para el diseño e implementación de controles de seguridad de los

cuales se derivan las acciones que deben tomar para evitar la materialización de riesgos.

En esta norma se especifican las acciones que deben ser tenidas en cuenta por las organizaciones para una óptima implementación de un SGSI en su interior. Para el cumplimiento de dichas acciones el compromiso de la alta dirección juega un papel muy determinante apoyando al destinar los recursos necesarios tantos económicos, de personal, capacitando al personal generando conciencia para la protección de los activos de información.

La norma también presenta las recomendaciones necesarias para la definición de los objetivos buscados con la implementación de un SGSI, el campo de aplicación, contexto, planificación, evaluación, mantenimiento, mejora y sostenibilidad del SGSI.

La norma en su Anexo A presenta en 14 dominios los 113 controles que sirven como referencia a las organizaciones para su implementación y garantizar así la seguridad en la ejecución de sus procesos con el propósito de reducir las vulnerabilidades y por ende impedir la materialización de amenazas que pongan en riesgo sus activos de información.

En cuanto al funcionamiento de las instituciones educativas en Colombia debemos referirnos a las siguientes:

Ley general de educación 115 de 1994 La ley general de Educación y los derechos reglamentarios regulan particularmente la prestación del servicio educativo tanto oficial como privado.

Decreto 1290 de 2009 Por el cual se reglamenta la evaluación del aprendizaje y promoción de los estudiantes.

El decreto 1860 define las características y condiciones para organizar y desarrollar los procesos que hacen posible la prestación del servicio educativo. En particular hace énfasis en la formulación y adopción de PEI. El gobierno escolar, como instancia de participación, las orientaciones para la evaluación y promoción del estudiante, la formulación de currículo y el calendario escolar.

En lo referente a la tipificación los delitos informáticos que establecen la protección de la información y de datos en Colombia, debemos referirnos a:

Ley 1273 de 2009 "*Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelable – 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".*

Decreto 1360 de 1989, *"De conformidad con lo previsto en la ley 23 de 1982 sobre Derechos de Autor, el soporte lógico (software) se considera como una creación propia del dominio literario. El soporte lógico (software) comprende uno o varios de los siguientes elementos: el programa de computador, la descripción de programa y el material auxiliar".*

Ley 527 de 1999 *"Con el cual se buscaba definir y reglamentar el acceso y uso del* comercio *electrónico, de las firmas digitales y se autorizaban las entidades de certificación y otras disposiciones"*.

Decreto 1747 de 2000 *"que reglamenta parcialmente la ley 527 de 1999 con lo relacionado a las entidades de certificación, los certificados y las firmas digitales".*

En lo relacionado con la protección de los datos personales y teniendo en cuenta que uno de los enfoques para la realización de este proyecto es el de garantizar el seguro resguardo de los datos personales tanto de alumnos, padres de familia y de los profesionales pertenecientes a la institución educativa colegio PRO-COLOMBIANO, es por esto que es de vital importancia referirse las leyes aplicables de acuerdo a la legislación colombiana en este aspecto, estas se enumeran a continuación.

Constitución Política de Colombia

TITULO II. DE LOS DERECHOS, LAS GARANTÍAS Y LOS DEBERES.
CAPITULO 1. DE LOS DERECHOS FUNDAMENTALES

ARTICULO 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las *informaciones* que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

Ley 527 del **18 de Agosto de 1999** donde se reglamenta el acceso y uso de los mensajes de datos, comercio electrónico y firmas digitales.

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.

Ley 1581 de 2012: La ley de protección de datos personales – es una ley que *complementa* la regulación vigente para la protección del derecho fundamental que tienen todas las personas naturales a autorizar la información personal que es almacenada en bases de datos o archivos, así como su posterior actualización y rectificación. Esta ley se aplica a las bases de datos o archivos que contengan datos personales de personas naturales.

En su *artículo* 28 estableció un plazo de 6 meses para la implementación y adaptación de políticas por parte de las empresas que hagan las veces de encargados y/o responsables del tratamiento de datos.

Decreto 1377 del 27 de junio de 2013: tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.

Reglamenta aspectos relacionados con la autorización del titular de la *información* para el tratamiento de sus datos personales, las políticas de tratamiento de los responsables y encargados, el ejercicio de los derechos de los titulares de la información, entre otros:

1. El anuncio como tal (y a los cinco días siguientes de la comunicación, enviar carta comunicándole al respecto a la Superintendencia de Industria y Comercio).
2. Formato de autorización para que si lo desean lo diligencien los titulares de datos recolectados previamente.
3. Determinación de canal electrónico y físico para recibir las autorizaciones.
4. Política de tratamiento de la información personal (pues esta se debe indicar en el anuncio).
5. Conducto regular y canales físicos y electrónicos definidos para que el titular ejerza sus derechos de acceso, rectificación y supresión. [6]

[6] **ABC para proteger los datos personales, Ley 1581 de 2012 Decreto 1377 de 2013**

6. MARCO METODOLÓGICO

6.1. METODOLOGÍA DE INVESTIGACIÓN

Para el desarrollo de este proyecto la metodología de investigación a utilizar es la aplicada, ya que esta por definición “es la que se apoya en la solución de problemas específicos para mejorar la calidad de vida de las sociedades, destinados a determinar las posibles causas de estos y poder evidenciar los hallazgos, mediante la realización de actividades, para así con los resultados obtenidos buscar la aplicabilidad de potenciales soluciones.

Es así que para el caso particular motivo de este proyecto en el cual se busca mediante la implementación de un SGSI en el colegio PRO-COLOMBIANO al determinar las amenazas, vulnerabilidades e identificación de los riesgos presentes en el los activos de información, para así con la determinación de las causas poder implementar controles y salvaguardas con el propósito de proteger los activos de información de los procesos de matrículas y manipulación de calificaciones.

6.2. METODOLOGÍA DE DESARROLLO

Las etapas a desarrollar en el proyecto se basan en los objetivos específicos, de los cuales se derivan las actividades a ejecutar, para lo cual al inicio de las actividades definidas en el cronograma de actividades se realizará reunión con las directivas de la institución para definir los integrantes del comité del SGSI y corroborar los alcances del proyecto.

6.2.1. Objetivo 1.

Con el propósito de definir los alcances del SGSI se deben establecer los activos de información, de infraestructura tecnológica y sistemas de información que existen en el colegio PRO-COLOMBIANO

Para el cumplimiento de este objetivo se realizaran las siguientes actividades:

- Reunión preliminar con las directivas de la institución e integrantes del comité SGSI con el propósito de conocer el organigrama y dependencias donde se puedan identificar los activos de información de la institución.

- Realizar entrevistas, cuestionarios, listas de chequeo a los empleados y directivas de la institución con el propósito de identificar los activos de información.

- Valorar activos de información identificados de acuerdo a la metodología utilizada (Magerit).

6.2.2. Objetivo 2.

Programar un plan de pruebas a llevar a cabo en el Colegio PRO-COLOMBIANO, para así determinar el nivel de seguridad en que se encuentra la institución.

Para el cumplimiento de este objetivo se realizaran las siguientes actividades:

- Coordinar con las directivas de la institución fechas y procesos a los que se puedan realizar las pruebas, teniendo en cuenta que no se afecte el normal funcionamiento de las actividades ejecutadas en la institución.

- Recolectar y analizar los resultados de las pruebas.

6.2.3. Objetivo 3.

Identificar las vulnerabilidades amenazas y riesgos existentes en la seguridad de la información, con el propósito de valorar el o los posibles impactos y probabilidad de ocurrencia de estos en lo concerniente a la confidencialidad, integridad y disponibilidad de la información.

Para el cumplimiento de este objetivo se realizaran las siguientes actividades:

- Identificar las amenazas y vulnerabilidades presentes en los activos identificados, las cuales se presentarán en cuadros tabulando esta información.

- Valorar las amenazas identificadas.

- Determinar impacto sobre los activos.

- Determinar riesgos potenciales a partir del análisis de las amenazas
- Determinar causas que producen los riesgos.

- Determinar niveles de riesgo aceptable y riesgo residual.

6.2.4. Objetivo 4.

Diseñar un manual del SGSI de acuerdo a los resultados anteriores que contenga las políticas y procedimientos de control de la seguridad a establecer en el Colegio PRO-COLOMBIANO.

Para el cumplimiento de este objetivo se realizaran las siguientes actividades:

- Definir el o los objetivos buscados al definir las políticas y procedimientos incluidos en el manual del SGSI a diseñar para el colegio PRO-COLOMBIANO.

- Definir la aplicabilidad del manual a diseñar.

- Elaborar políticas de Seguridad.

- Revisión y análisis de políticas definidas.

- Presentar conclusiones, resultados y entrega de manual a las directivas de la institución.

- Despejar dudas, impartir instrucciones sobre la aplicabilidad e implementación de los controles sugeridos.

7. PLAN DE TRATAMIENTO DE RIESGOS

El desarrollo de los objetivos planteados se cimenta en base a lo establecido la recomendación ISO 27001, por medio del uso del ciclo continuo PHVA (Planear – Hacer – Verificar – Actuar, para lo cual se define que en cada ciclo se realiza:

- **Planear**: establecer el SGSI.
- **Hacer**: implementar y utilizar el SGSI.
- **Verificar**: monitorear y revisar el SGSI.
- **Actuar**: mantener y mejorar el SGSI.

FASE DE PLANEACIÓN DEL SGSI

- Determinar del alcance del SGSI.
- Redactar la una Política de SGSI.
- Identificar la metodología de evaluación de riesgos y determinar los criterios para la aceptabilidad de riesgos.
- Identificar activos, vulnerabilidades y amenazas.
- Evaluar la magnitud de los riesgos.
- Identificar y evaluar opciones para el tratamiento de riesgos.
- Seleccionar controles para el tratamiento de riesgos.
- Obtener la aprobación de la gerencia para los riesgos residuales.
- Obtener la aprobación de la gerencia para la implementación del SGSI.
- Redactar una declaración de aplicabilidad que detalle todos los controles aplicables y determine cuáles ya se han implementados y cuáles no son aplicables.

De acuerdo a lo anterior se inicia con la fase “Planear” del ciclo PHVA que para el proceso de este proyecto implica determinar los alcances del mismo, en este sentido es fundamental contar con el compromiso de la alta dirección la cual debe entender que la implementación de un SGSI va en concordancia y alineada con los objetivos organizacionales.

7.1. ALCANCES

El alcance definido para la implementación del sistema de gestión de seguridad de la información en la institución educativa colegio PRO-COLOMBIANO está enfocado a los procesos de matrícula y procesamiento de las calificaciones de los alumnos de la institución.

7.1.1. Población

El proyecto se concreta a la ciudad de Bogotá, en la sede del colegio PRO-COLOMBIANO.

7.1.2. Muestra

Se tendrá en cuenta el 100% de la población con acceso a los procesos de generación actualización de las calificaciones de los alumnos de la institución, y datos personales tanto de alumnos y funcionarios de la institución.

Es así que habiendo establecidos los alcances y mediante reunión con las directivas de la institución para la conformación de un comité SGSI (ver Anexo B) y asignación de personal de apoyo para el desarrollo del proyecto, se procede al desarrollo del primer objetivo planteado

*"*Establecer *los activos de información, de infraestructura tecnológica, sistemas de información e información que existen en el colegio PRO-COLOMBIANO con el propósito de definir los alcances del SGSI"*

7.2. METODOLOGÍA A UTILIZAR PARA EVALUACIÓN DE RIESGOS

7.2.1. Selección de Metodología.

El desarrollo de este proyecto, se fundamenta en la metodología Magerit, la cual especifica varias etapas que se describen a continuación:

1. Identificación y Valoración de Activos (relevantes): Determinar los activos que existen en la entidad en este caso el colegio PRO-COLOMBIANO, estableciendo tipo y asignándoles un valor,

2. Identificación y Valoración de Amenazas: Identificar amenazas latentes, estableciendo niveles de peligro a la que están expuestos los activos y que los puedan llegar a afectar, asimismo realizar una valoración de las vulnerabilidades al identificar la frecuencia de ocurrencia o materialización con que se presente o se halla presentada una amenaza.

3. Estimación de Impacto: Establecer el nivel del daño causado o que pudiera llegar a causarse en el supuesto de materializarse las amenazas registradas en los activos identificados.

4. Identificación de controles o salvaguardas: Identificar que controles se encuentran instituidos determinando su eficacia para la mitigación de riesgos.

5. Determinación del riesgo efectivo: Estimar el riesgo luego dela aplicación de las salvaguardas.

7.3. IDENTIFICACIÓN DE ACTIVOS

Un activo de información para el colegio PRO-COLOMBIANO es todo aquel elemento que contiene o manipula información.

Magerit establece como activos relevantes

- Datos que materializan la información.
- Servicios auxiliares que se necesitan para poder organizar el sistema.
- Las aplicaciones informáticas (software) que permiten manejar los datos.
- Los equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y servicios.
- Los soportes de información que son dispositivos de almacenamiento de datos.
- El equipamiento auxiliar que complementa el material informático.
- Las redes de comunicaciones que permiten intercambiar datos.
- Las instalaciones que acogen equipos informáticos y de comunicaciones.
- Las personas que explotan u operan todos los elementos anteriormente citados.[7]

De acuerdo a lo establecido con la alta dirección de la institución en reunión efectuada para la conformación del comité SGSI (ver Anexo B), se estableció que para el levantamiento de la información se procede mediante el método de visitas a las instalaciones y realización de entrevistas personales a los encargados de los procesos con el fin de determinar el inventario de activos presentes.

En el proceso de caracterización de los activos de información presentes en la institución fue fundamental la colaboración de su rectora y propietaria, quien identificó, valoró y suministró para los propósitos de este proyecto los activos de información presentes en el colegio PRO-COLOMBIANO, información que se utilizó como insumo para el desarrollo de las fases propuestas en la metodología Magerit.

En la Tabla 2 se muestra la identificación de los activos de información que propone Magerit.

[7] Tomado de Magerit v_3 Libro 1.0

Tabla 2. Categorías de los activos de información

CATEGORIAS DE LOS ACTIVOS DE INFORMACIÓN		
Identificador	**Categoría**	**Ejemplos**
DAT	Datos / información	BD, archivos de datos, contratos y acuerdos, documentación del sistema, información de investigación, manuales de usuario, material de entrenamiento, de operación, procedimientos de soporte, planes de continuidad y contingencia, acuerdos
SW	Software / Aplicaciones	Aplicaciones, sistemas operativos, herramientas de desarrollo y utilitarios
HW	Hardware / equipos Servidores (S.O.)	PCs, routers, hubs, firewalls.
SI	Soportes de información.	SAN, discos, cintas, USB, CD, DVD
COM	Redes de comunicaciones	Medios de transporte que llevan datos de un sitio a otro
AUX	Equipamiento auxiliar	Equipamiento de soporte a los sistemas de información (UPS, Generados, Aire acondicionado, cableado, etc.)
PER	Personal / RR.HH.	Personas, calificaciones, experiencia y capacidades (usuarios, proveedores, personal de TI)
INS	Locales / Instalaciones	Lugares donde se hospedan los sistemas de Información, registros vitales y comunicaciones

Fuente: El autor

En la Tabla 3 se presenta el inventario de activos identificados en el colegio PRO-COLOMBIANO

Tabla 3. Identificación de activos Colegio PRO-COLOMBIANO

Categoría Magerit	**Activo**	**Cantidad**	**Descripción de activos**
DAT	Información	N/A	Informe académico periódico
		N/A	Informe certificado de notas
		N/A	Sabana de notas
		N/A	Hojas de matriculas
		N/A	Libro consolidado de matriculas
		N/A	Libro consolidado de notas
		N/A	Archivo hojas de vida alumnos

Categoría Magerit	Activo	Cantidad	Descripción de activos
		N/A	Archivo hojas de vida empleados
		N/A	Observador del estudiante
SW	Software	1	Antivirus (licencia McAfee)
		1	Sistema operativo Microsoft Windows 8 Professional
		1	Microsoft Office
HW	Hardware	3	Computadores portátiles
		2	Computadores de escritorio
		1	Router / Hub
SI	Soportes de información	2	Memorias USB
		1	Disco duro externo
COM	Red	N/A	Internet
		N/A	Red telefónica
		N/A	Conexión inalámbrica
AUX	Equipamiento auxiliar	4	Sistemas de extinción de incendios
PER	Personas	N/A	Funcionarios de planta
		N/A	Contratistas
		N/A	Proveedores
		N/A	Partes interesadas (entidades públicas),
INS	Infraestructura	N/A	Archivo
		N/A	Sala de informática
		N/A	Sala rectoría
	Intangibles	N/A	Imagen y reputación
		N/A	Conocimiento
		N/A	Ideas

Fuente: El autor

7.4. VALORACIÓN DE ACTIVOS

Teniendo identificados los activos disponibles al interior del colegio PRO-COLOMBIANO el siguiente paso a ejecutar de acuerdo a la metodología seleccionada corresponde a la valoración de estos.

La metodología Magerit en su versión 3 Libro 1 Método, numeral 3.1.1 página 24 de 127 “Dimensiones” establece que de un activo puede interesar valorar diferentes dimensiones:

- Su confidencialidad: ¿qué daño causaría que lo conociera quien no debe? Esta valoración es típica de datos.
- Su integridad: ¿qué perjuicio causaría que estuviera dañado o corrupto? Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcialmente falsos o, incluso, faltar datos.
- Su disponibilidad: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo?

Magerit establece que una vez determinadas las dimensiones (de seguridad) que se definen para un activo de información, hay que proceder a valorarlo. La valoración es la determinación del coste que supondría recuperarse de una incidencia que destrozara dicho activo. Los factores que establece la metodología Magerit en su versión 3 Libro 1 Método, numeral 3.1.1 página 25 de 127 “¿Cuánto vale la salud de sus activos?”, establece que las acciones a considerar son:

- Coste de reposición: adquisición e instalación
- Coste de mano de obra (especializada) invertida en recuperar (el valor) del activo
- Lucro cesante: pérdida de ingresos
- Capacidad de operar: confianza de los usuarios y proveedores que se traduce en una pérdida de actividad o en peores condiciones económicas
- Sanciones por incumplimiento de la ley u obligaciones contractuales
- Daño a otros activos, propios o ajenos
- Daño a personas Daños medioambientales [8]

Teniendo determinado los factores por los cuales se valoran los activos, se establece una escala de valoración cualitativa y cuantitativa, para la cual se tiene en cuenta la relevancia de cada activo para la institución la cual es establecida por las directivas de la institución y que se presenta en la Tabla 4 (Criterios de valoración de activos).

[8] Magerit V3 Libro1 Método

Tabla 4. Criterios de valoración de activos

Escala valoración	Valor cualitativo	Escala cuantitativa en millones	Descripción
MB: Muy bajo	1	0 a10	Irrelevante para efectos Prácticos
B: Bajo	2	10 a 50	Importancia menor para la empresa
M: Medio	3	50 a 100	Importante para la empresa
A: Alto	4	100 a 200	Altamente importante para la empresa
MA: Muy alto	5	Más de 200	De vital importancia para los objetivos que busca la empresa

Fuente: El autor

Habiendo definido los criterios para valorar los activos, se presenta la información en la Tabla 5 (Valoración de activos colegio PRO-COLOMBIANO)

Tabla 5. Valoración de activos colegio PRO-COLOMBIANO

Identificación	Descripción	Valoración activos		
		Confidencialidad	Integridad	Disponibilidad
	Informe académico periódico	5	5	5
	Informe certificado de notas	5	5	5
	Sabana de notas	5	5	5
	Hojas de matriculas	5	5	5
	Libro consolidado de matriculas	5	5	5
	Libro consolidado de notas	5	5	5
	Archivo hojas de vida funcionarios	5	5	3

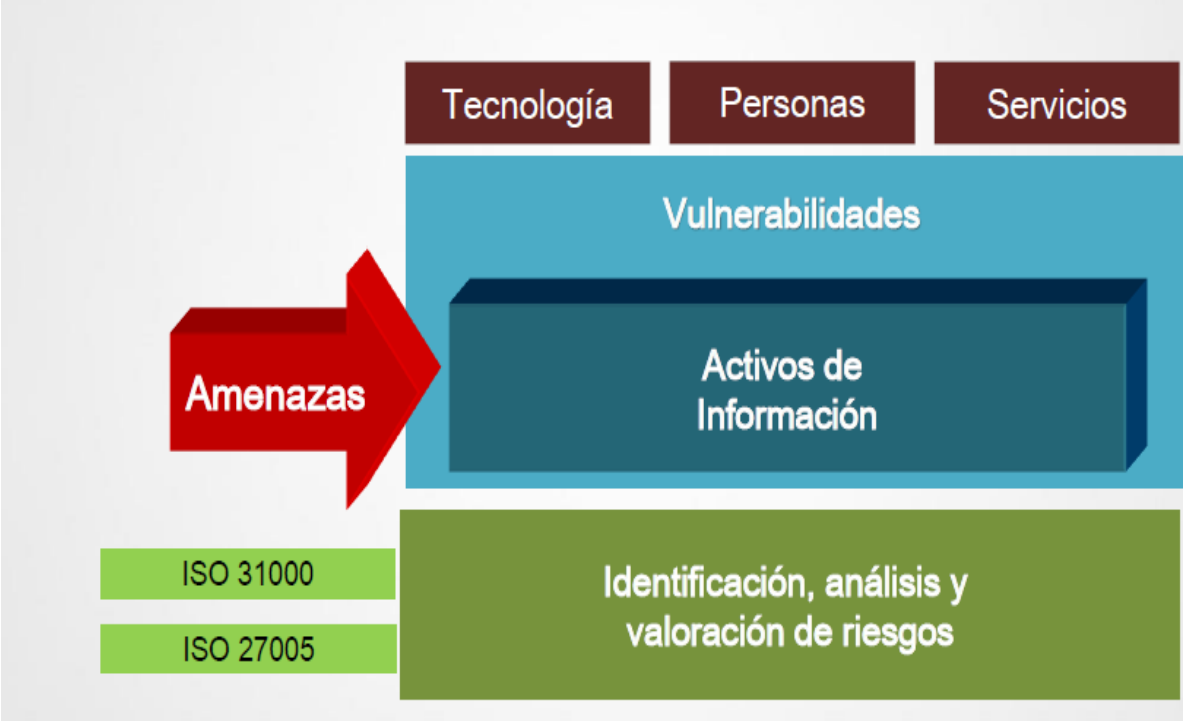
Identificación	Descripción	Valoración activos		
		Confidencialidad	Integridad	Disponibilidad
	Archivo hojas de vida alumnos	5	5	4
	Observador del estudiante	5	5	3
Herramientas de Seguridad Perimetral	Licencias de McAfee	4	4	4
	Licencias Antivirus	4	4	4
Sistema Operativo	Microsoft® Windows 8	5	4	3
Aplicaciones de Oficina	Microsoft® Office	5	4	4
Computadores	Portátiles	5	4	4
	De Escritorio	5	4	4
Cuarto de Computo	Sala de Informática	5	5	5
Archivo	Rectoría	5	5	5
Comunicaciones	Modem - router	4	4	5
Dispositivos de comunicación - Móviles y otras	Teléfonos Celulares	4	4	3
	Telefonía fija	4	4	3
Internet	Claro	4	4	5
Navegador web	Chrome, Mozilla, Explorer	3	3	3
Correo electrónico	Mail personal	5	5	3
Jefe Telemática	Licenciado área sistemas	5	5	5
Generadores de información	Licenciados, alumnos, padres de familia	5	5	5
Imagen y reputación	Percepción de los clientes de la institución	4	4	4
Conocimiento	Información que poseen los funcionarios	5	5	5

Fuente: El autor

7.5. MÉTODO DE ANÁLISIS DE RIESGOS

La metodología a seguir para el análisis de riesgos es identificar, evaluar, tratar y monitorear los riesgos de la información definiendo los niveles aceptables de riesgo según las norma ISO/IEC 27001, ISO 31000, lo cual se comprende mejor al observar la Figura 9.

Figura 9. Gestión de riesgos ISO 27001



Fuente: Servicio Nacional de Aprendizaje – SENA

Análisis y Evaluación de Riesgos de Seguridad de la Información

- ✓ Identificación de las amenazas
- ✓ Identificación de las vulnerabilidades
- ✓ Identificación de los Riesgos
- ✓ Selección de la Probabilidad de Ocurrencia
- ✓ Determinar el impacto en los Activos de Información
- ✓ Valoración del Riesgo Inherente
- ✓ Identificación de controles existentes
- ✓ Definición de los niveles de aceptación de Riesgos

Previo al proceso de identificación de las amenazas y vulnerabilidades que puedan afectar a los activos de información del colegio PRO-COLOMBIANO, se consideró

necesario diseñar y programar un plan de pruebas con el propósito de verificar las medidas que en cuanto a seguridad tiene implementada la institución para proteger sus activos de información.

El plan de pruebas diseñado y los procesos llevados a cabo se describen en el numeral 7.5.1

7.5.1. Plan de pruebas

En esta etapa del proyecto se define un plan de pruebas ajustado al cronograma de actividades previamente establecido (ver Anexo F) y teniendo como base los procesos llevados a cabo en el colegio descritos en el capítulo 5 inciso 5.2.5; se define un plan en el cual se determina la realización actividades y de pruebas que incluye:

Tabla 6. Plan de pruebas propuesto

ACTIVIDADES	OBJETIVO	ACTIVIDADES EJECUTADAS
Pruebas de recorrido	• Familiarización con los procesos y actividades llevadas a cabo en la institución • Conocer la documentación utilizada en la institución para el desarrollo de las actividades propias de esta.	• Acompañamiento al proceso de inscripción de estudiantes, matrículas y legalización de matrículas. • Acompañamiento al personal docente en el proceso de calificaciones, procesamiento de información, llenado de formatos y entrega para consolidación y construcción de boletines de calificaciones • Acompañamiento en el proceso de reportes y subida de información al SIMAT • Acompañamiento y observación en el proceso de

		digitalización de información. • Acompañamiento y observación en el proceso de archivo de la información.
Replica y simulación de los procesos	Conocer los procesos y procedimientos llevados a cabo por las directivas y colaboradores de la institución con el propósito de evaluar las falencias que pongan en riesgo la seguridad de los activos de información	• En un ambiente controlado realizar acompañamiento y replicar las actividades que se ejecutan y que implican manipulación de información. • Verificar si existen procedimientos establecidos para garantizar la seguridad de los activos de información.
Idealización y discusión de situaciones críticas que puedan afectar los procesos.	Poner en contexto las situaciones que generan riesgo a los activos de información de la institución.	• Ejecución de reuniones en donde se discuten los eventos y situaciones que pueden generar brechas de seguridad en los procesos de manipulación de información y de los activos de información
Recopilación de información y construcción de Tablas y matrices que recojan los resultados obtenidos	Presentación de resultados para análisis y posterior identificación de amenazas y vulnerabilidades que puedan llegar a afectar los activos de información identificados en la institución.	• Consolidación de información y elaboración de tabla donde se presentan las falencias y debilidades presentes en la institución.

Fuente: El autor

Como resultado de las actividades ejecutadas en el plan de pruebas desarrollado, se obtuvieron los datos que definen el nivel de seguridad en el cual se encuentra la institución, las debilidades que presentan sus procesos y que pueden conllevar a la materialización de amenazas que pongan en riesgo los activos de información identificados en el colegio PRO-COLOMBIANO.

Esta información es presentada en la Tabla 7. (Debilidades identificadas en los procesos)

Tabla 7. Debilidades identificadas en los procesos

PROCESO	DEBILIDADES IDENTIFICADAS
Matriculas	• La información recibida no es foliada • La información recibida de los alumnos es almacenada en la sala de archivo, se evidenció que esta sala permanece abierta sin vigilancia. • La puerta acceso a la sala de archivo no cuenta con cerradura de seguridad. • La información recibida en medio físico no es digitalizada inmediatamente, es almacenada en la sala de archivos. • El computador donde es almacenada la información de los alumnos matriculados no cuenta con clave de inicio de sesión, adicional a que solo se encuentra un solo usuario configurado el cual cuenta con todos los privilegios tanto de escritura como de modificación
Calificaciones	• El computador donde es almacenada la información de los alumnos matriculados no cuenta con clave de inicio de sesión, adicional a que solo se encuentra un solo usuario configurado el cual cuenta con todos los privilegios tanto de escritura como de modificación. • No existe un procedimiento definido que avale la entrega oportuna de los formatos de calificaciones por parte de los docentes de la institución. • No existe un formato en donde se registre un histórico de modificaciones de los formatos de calificaciones en caso de que esto se requiera.
Procesamiento de información	• No existe back up de la información. • Los computadores donde se almacena la información no cuentan con asignación de usuarios y roles. • No existen claves asignadas a los usuarios para el uso de computadores.
Administrativos	• En los contratos de los funcionarios, no se incluyen cláusulas de confiabilidad de la información confidencial que manipulen en el desarrollo de sus labores.

	• No existe un manual que defina los procedimientos para el manejo y la protección de la información confidencial. • El personal no ha sido capacitado en aspectos relativos a la protección de la información confidencial, • La institución no cuenta con un seguro para protección contra riesgos. • No existe un registro de eventos ni las medidas ejecutadas que registre los eventos que afectaron los activos de información de la institución. • No existe sistema de cámaras de vigilancia. • No existe un plan de mantenimiento preventivo destinado a los equipos que contienen la información confidencial. • No existe un plan de contingencia ni de continuidad del negocio.

Fuente: el autor

7.6. IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

Para este proceso se consideró fundamental poner en contexto a las directivas de la institución las diferentes fuentes que pueden originar las amenazas y vulnerabilidades que puedan afectar a los activos de información en una organización y que se describen a continuación

- Errores de operación accidental. Causados por las personas que operan el sistema a todos los niveles.
- Ataques deliberados. Causados por personas, usuarias o no del sistema, de forma intencional.
- Defectos del software. Defectos técnicos de diseño, implementación del software.
- De origen natural como terremotos, incendios o inundaciones.
- De origen industrial como la contaminación, fallas eléctricas, escapes de agua o gas, fallas eléctricas.

Como resultado de estas pruebas se obtuvieron los siguientes resultados en donde se identifican las causas que conllevan a la posible materialización de amenazas y vulnerabilidades que puedan afectar y poner en riesgo a los activos de información de la institución educativa colegio PRO-COLOMBIANO.

En la Tabla 8 (Identificación de amenazas y vulnerabilidades asociadas a los activos) se presenta el consolidado de las amenazas y vulnerabilidades para el colegio PRO-COLOMBIANO, como consecuencia de las debilidades identificadas en los procesos llevados a cabo en la institución, las cuales se encuentran consignadas en la Tabla 7 (Debilidades identificadas en los procesos) previa verificación de las actividades y procesos desarrollados en la institución, los cuales se encuentran descritos en el capítulo 5 incisos 5.2.5 y a las pruebas realizadas a cada proceso y a la ejecución de las actividades establecidas en el plan de pruebas.

Tabla 8. Identificación de amenazas y vulnerabilidades asociadas a los activos

Activo	Descripción de activos	Amenazas	Vulnerabilidades
Información	Informe académico periódico Informe certificado de notas Sabana de notas Hojas de matriculas Libro consolidado de matriculas Libro consolidado de notas Archivo hojas de vida alumnos Archivo hojas de vida empleados Observador del estudiante	• Código malicioso (troyanos, gusanos, virus, entre otros) • Incumplimiento de políticas o procedimientos internos. • Daño accidental (incendio, agua, humedad, contaminación química, construcción, entre otros) • Ataques maliciosos (vandalismo, hurto,). • Uso no autorizado de recursos (equipos de comunicación, medios de almacenamiento, sistemas de información, computadores). • Acceso no autorizado a la información o a las instalaciones (oficinas, edificio, sala, centro de cómputo, etc.) • Intrusión o acceso forzado (instalaciones, sistemas de información, información).	• Falta de segregación de funciones o incorrecta aplicación de las mismas. • Acceso no controlado a información sensible confidencial. • Ausencia o insuficiencia de políticas, procedimientos y directrices de seguridad. • Documentación insuficiente o desactualizada. • Eliminación de información sin borrado o destrucción segura. • Ausencia o insuficiencia de copias de respaldo. • Ausencia o insuficiencia de un proceso para clasificar y etiquetar la información. • Ausencia o insuficiencia de contratos, acuerdos de niveles de servicio y/o confidencialidad

Activo	Descripción de activos	Amenazas	Vulnerabilidades
		• Hurto o robo (información, documentos, medios o equipos). • Divulgación no autorizada.	con empleados o terceros. • Descarga y/o uso no controlado de software. • Uso de software ilegal /No autorizado/ software malicioso. • Ausencia de control de los activos que se encuentran fuera de las instalaciones. • Ausencia o insuficiencia de procedimientos de monitoreo de los recursos de procesamiento de información.
Software	Antivirus (licencia McAfee) Sistema operativo Microsoft Windows 8 Professional Microsoft Office	• Código malicioso (troyanos, gusanos, bomba lógica, entre otros). • Falla o mal funcionamiento del Software • Errores de transmisión o almacenamiento. • Ataques contra el sistema (negación del servicio, manipulación de software, manipulación de equipo informático, entre otros). • Uso de software no licenciado o no autorizado.	• Especificaciones o requerimientos incompletos, inadecuados o no claros. • Ausencia o insuficiencia en el control de los activos que se encuentran fuera de las instalaciones. • Arquitectura insegura de la red. • Ausencia o insuficiencia de mantenimiento. • Almacenamiento de equipos sin protección. • Fallas o degradación de equipos. • Disposición o reutilización de medios de almacenamiento sin borrado seguro. • Canales de comunicación sin encripción.

Activo	Descripción de activos	Amenazas	Vulnerabilidades
			• Ausencia de sistemas y/o procedimientos de monitoreo de la red. • Ausencia o insuficiencia de pruebas. • Ausencia o insuficiencia de actualizaciones. • Faltas conocidas o defectos del software. • Ausencia de logs o registros de auditoría. • Configuraciones por defecto. • Ausencia o insuficiencia de documentación de uso y/o administración. • Ausencia o insuficiencia de mecanismos de identificación y autenticación. • Puertos o servicios activos no requeridos. • Descarga y/o uso no controlado de software. • Ausencia o insuficiencia de copias de respaldo. • Eliminación de información sin borrado seguro.
Hardware	Computadores portátiles Computadores de escritorio Routers Hubs	• Falla o mal funcionamiento del hardware. • Avería de origen físico o lógico • Perdida de equipos	• Especificaciones o requerimientos incompletos, inadecuados o no claros. • Ausencia o insuficiencia en el control de los activos que se encuentran dentro y fuera de las instalaciones. • Ausencia o insuficiencia de

Activo	Descripción de activos	Amenazas	Vulnerabilidades
			mecanismos de identificación y autenticación. • Falta de mantenimiento a los equipos. • Ausencia o insuficiencia de documentación de uso y/o administración.
Soportes de información	Memorias USB Disco duro externo	• Intrusión o acceso forzado (instalaciones, sistemas de información, información). • Hurto o robo (información, documentos, medios o equipos). • Divulgación no autorizada. • Incumplimiento de políticas o procedimientos internos. • Daño accidental (incendio, agua, humedad, contaminación química, construcción, entre otros)	• Ausencia o insuficiencia de documentación de uso y/o administración • Ausencia o insuficiencia de mecanismos de identificación y autenticación. • Ausencia o insuficiencia en el control de los activos que se encuentran dentro y fuera de las instalaciones.
Redes de telecomunicaciones	Internet Red telefónica Red inalámbrica	• Falla o mal funcionamiento • Avería de origen físico o lógico • Perdida de equipos • Falla sistema de comunicaciones (Internet).	• Falta de mantenimiento a los equipos. • Ausencia o insuficiencia de documentación de uso y/o administración.
Equipamiento auxiliar	Sistemas de extinción de incendios (extinguidores)	• Falla o mal funcionamiento • Avería • Perdida de información	• Falta de mantenimiento a los equipos. • Ausencia o insuficiencia de documentación de uso y/o administración.

Activo	Descripción de activos	Amenazas	Vulnerabilidades
			• Falta capacitación en el uso en caso de emergencia
Personas	Funcionarios de planta Contratistas Proveedores Partes interesadas (entidades públicas),	• Intruso externo (Ej. exempleado, delincuente informático, interesados. • Empleados (acciones involuntarias y/o deliberadas). • Proveedor o contratista. • Uso no autorizado de recursos (equipos de comunicación, medios de almacenamiento, sistemas de información, computadores. • Manipulación del sistema. • Espionaje (ingeniería social). • Abuso de derechos (de usuario, de administrador). • Acceso no autorizado a la información o a las instalaciones (oficinas, edificios, archivo, sala de cómputo, • Intrusión o acceso forzado (instalaciones, sistemas de información, información). • Hurto o robo (información, documentos, medios o equipos). • Error en el uso (de equipos, medios, información, sistemas o servicios de información).	• Acceso no contralado a información sensible / confidencial. • Ausencia de mecanismos de monitoreo a la actividad de los empleados y/o terceros. • Ausencia o insuficiencia de cláusulas contractuales y/o acuerdos de confidencialidad. • Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos, con los empleados y/o terceras partes. • Ausencia o insuficiencia de políticas, procedimientos y/o directrices de seguridad. • Ausencia o insuficiencia en la definición y formalización de roles, funciones y responsabilidades. • Dependencia de personal clave, ausentismo o personal insuficiente. • Desconocimiento, malinterpretación o no cumplimiento de las disposiciones legales, contractuales y/o regulatorias aplicables.

Activo	Descripción de activos	Amenazas	Vulnerabilidades
			• Falta de segregación de funciones o incorrecta aplicación de las mismas. • Incumplimiento de políticas o procedimientos internos. • Insuficiente entrenamiento, capacitación o sensibilización.
Infraestructura	Archivo Sala de informática Sala rectoría	• Ataque malicioso (terrorismo, vandalismo, hurto). • Desastre natural (temblor, terremoto, inundación, incendio,). • Daño accidental (incendio, agua, humedad).	• Ausencia o insuficiencia de controles de acceso a las instalaciones. • Ausencia o insuficiencia de controles de monitoreo de las instalaciones (por ejemplo, detección o extinción de incendios, líquidos inflamables, CCTV, entre otros. • Ausencia o insuficiencia de planes de emergencia y simulacros de evacuación. • Falta en los servicios esenciales (internet, teléfonos) • Ausencia o insuficiencia de mantenimiento preventivo / correctivo.
Intangibles	Imagen y reputación Conocimiento Ideas	• Incumplimiento de leyes o regulaciones (propiedad intelectual entre otros). • Uso no autorizado de recursos (equipos de comunicación, medios de	• Ausencia de responsables sobre la gestión en seguridad de la información y/o continuidad de negocio. • Ausencia de planes de continuidad.

Activo	Descripción de activos	Amenazas	Vulnerabilidades
		almacenamiento, sistemas de información, computadores). • Hurto o robo (información, documentos, medios o equipos). • Incumplimiento de políticas o procedimientos internos.	• Ausencia o insuficiencia de un proceso de gestión de incidentes de seguridad. • Ausencia o insuficiencia de un procedimiento para el manejo de comunicaciones externas.

Fuente: El autor

7.7. VALORACIÓN DE AMENAZAS

Teniendo identificadas las amenazas presentes y que pueden afectar a los activos del colegio PRO-COLOMBIANO se procede a valorar que influencia pueden tener estas en función de la degradación y probabilidad de ocurrencia, a continuación se describen estos conceptos para su valoración, para lo cual se toma como referencia lo especificado en la metodología Magerit.

Degradación: cuán perjudicado resultaría el [valor del] activo, mide el daño causado por un incidente en el supuesto de que ocurriera, ver Tabla 9.

Tabla 9. Criterios de valoración de amenazas (Degradación)

Degradación de activos			
Escala	**Valor**	**Frecuencia**	**En lapso de tiempo**
MB: Muy Bajo	1	Muy poco frecuente	En siglos
B: Bajo	2	Poco frecuente	En varios Años
M: Medio	3	Normal	En un año
A: Alto	4	Frecuente	En un mes
MA: Muy Alto	5	Muy frecuente	A diario

Fuente: El autor

Probabilidad: cuán probable o improbable es que se materialice la amenaza, esta valoración se presenta en la Tabla 10.

Tabla 10. Criterios de valoración de amenazas (Probabilidad de ocurrencia)

Probabilidad de ocurrencia			
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

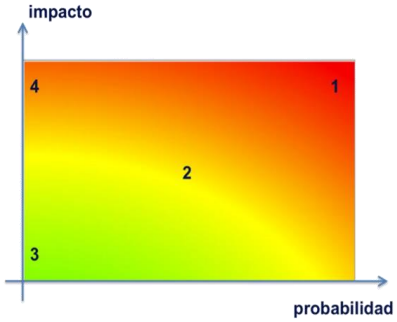
Fuente: El autor

Es conveniente definir las zonas a tener en cuenta para el tratamiento de los riesgos las cuales se determinan teniendo como criterios que el riesgo crece con el impacto y con la probabilidad.

De acuerdo a la metodología seleccionada (Magerit) estas zonas se definen así:

- Zona 1 Riesgos muy probables y de muy alto impacto
- Zona 2 Franja amarilla: cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables pero de impacto bajo o muy bajo.
- Zona 3 Riesgos improbables y de bajo impacto
- Zona 4 Riesgos improbables pero de muy alto impacto.

Figura 10. El riesgo en función del impacto y la probabilidad



Fuente: Magerit v3 Libro 1 Método

Teniendo como base las anteriores definiciones y aplicándolas a los activos identificados se genera una matriz la cual se presenta en la Tabla 11 (Valoración de amenazas).

Tabla 11 Valoración de amenazas

Activo	Amenazas	Influencia en el activo		Riesgo potencial
		Degradación	Probabilidad	
Información	Hurto o robo (información, documentos, medios o equipos).	MA	A	Zona 1
	Divulgación no autorizada	M	B	Zona 2
	Daño accidental (incendio, agua, humedad, contaminación química, construcción, entre otros)	M	B	Zona 2
	Ataques maliciosos (vandalismo, hurto,).	M	B	Zona 2
	Uso no autorizado de recursos (equipos de comunicación, medios de almacenamiento, sistemas de información.	M	B	Zona 2
	Acceso no autorizado a la información o a las instalaciones (oficinas, edificio, sala, centro de cómputo, etc.)	M	B	Zona 2
	Intrusión o acceso forzado (instalaciones, sistemas de información, información).	M	B	Zona 2
	Incumplimiento de políticas o procedimientos internos.	M	B	Zona 2
	Código malicioso (troyanos, gusanos, virus, entre otros)	M	B	Zona 2
Software	Código malicioso (troyanos, gusanos, bomba lógica, entre otros).	M	M	Zona 2
	Falla o mal funcionamiento del Software	M	M	Zona 2

Activo	Amenazas	Influencia en el activo		Riesgo potencial
		Degradación	Probabilidad	
	Errores de transmisión o almacenamiento.	A	M	Zona 1
	Ataques contra el sistema, manipulación de software, manipulación de equipo informático, entre otros).	B	B	Zona 3
	Uso de software no licenciado o no autorizado.	M	M	Zona 2
Hardware	Falla o mal funcionamiento del hardware.	M	M	Zona 2
	Avería de origen físico o lógico.	M	M	Zona 2
	Perdida de equipos	M	M	Zona 2
Soportes de información	Intrusión o acceso forzado (instalaciones, sistemas de información, información).	B	B	Zona 3
	Hurto o robo (información, documentos, medios o equipos).	M	M	Zona 2
	Divulgación no autorizada.	B	B	Zona 3
	Incumplimiento de políticas o procedimientos internos.	M	B	Zona 2
	Daño accidental (incendio, agua, humedad, contaminación química, construcción, entre otros)	B	B	Zona 3
Redes de telecomunicaciones	Falla o mal funcionamiento	M	M	Zona 2
	Avería de origen físico o lógico.	M	M	Zona 2
	Perdida de equipos	M	M	Zona 2

Activo	Amenazas	Influencia en el activo		Riesgo potencial
		Degradación	Probabilidad	
	Falla sistema de comunicaciones (Internet).	M	M	Zona 2
Equipamiento auxiliar	Falla o mal funcionamiento	B	B	Zona 3
	Avería	M	B	Zona 2
	Perdida de información	M	B	Zona 2
Personas	Intruso externo (Ej. exempleado, delincuente informático, interesados.	B	B	Zona 3
	Empleados (acciones involuntarias y/o deliberadas).	B	B	Zona 3
	Proveedor o contratista.	B	B	Zona 3
	Uso no autorizado de recursos (equipos de comunicación, medios de almacenamiento, sistemas de información, computadores.	B	B	Zona 3
	Manipulación del sistema.	B	B	Zona 3
	Espionaje (ingeniería social).	M	B	Zona 2
	Abuso de derechos (de usuario, de administrador).	M	B	Zona 2
	Acceso no autorizado a la información o a las instalaciones (oficinas, edificios, archivo, sala de cómputo,	M	M	Zona 2
	Intrusión o acceso forzado (instalaciones, sistemas de información, información).	B	B	Zona 3
	Hurto o robo (información, documentos, medios o equipos)	MA	M	Zona 4

Activo	Amenazas	Influencia en el activo		Riesgo potencial
		Degradación	Probabilidad	
	Error en el uso (de equipos, medios, información, sistemas o servicios de información).	M	M	Zona 2
Infraestructura	Ataque malicioso (terrorismo, vandalismo, hurto).	B	B	Zona 3
	Desastre natural (temblor, terremoto, inundación, incendio,).	B	B	Zona 3
	Daño accidental (incendio, agua, humedad).	B	B	Zona 3
Intangibles	Incumplimiento de leyes o regulaciones (propiedad intelectual entre otros).	MB	B	Zona 3
	Uso no autorizado de recursos (equipos de comunicación, medios de almacenamiento, sistemas de información, computadores).	M	B	Zona 2
	Hurto o robo (información, documentos, medios o equipos).	M	B	Zona 2
	Incumplimiento de políticas o procedimientos internos.	M	B	Zona 2

Fuente: El autor

7.8. SALVAGUARDAS

Es fundamental que las directivas del colegio PRO-COLOMBIANO estén enterados del nivel de riesgo que actualmente enfrentan, el cual se determina del análisis de las salvaguardas que actualmente estén implementadas y que se identifiquen

Las salvaguardas pueden ser (Funciones, Servicios y Mecanismos) que tiene como propósito representar una protección frente a las amenazas al limitar la frecuencia de ocurrencia, limitando y mitigando el impacto en caso de materializarse las

amenazas y el daño que estas puedan ocasionar y reduciendo el factor de degradación del valor de los activos.

Se procede a identificar las salvaguardas implementadas o que estén presentes en el colegio PRO-COLOMBIANO, estas se valoran de acuerdo a la Tabla 12 (Valoración de salvaguardas)

Tabla 12 Valoración de salvaguardas

Eficacia	**Madurez**	**Estado**
0% (L0)	No existe	No existe
10% (L1)	Iniciando	Iniciando
50% (L2)	Implementado	Parcialmente funcional
90% (L3)	En proceso	Funcional
95% (L4)	Medible	Es monitorizado
100%(L5)	Optimizado	En mejora continúa

Fuente: El autor

Teniendo como insumo la Tabla 12 (Valoración de salvaguardas), se procede a identificar las salvaguardas presentes en el colegio PRO-COLOMBIANO y a realizar su valoración, información que se presenta en la Tabla 13 (Identificación y valoración de salvaguardas), basándonos en la guía de salvaguardas establecidas en el libro II catálogo de elementos Magerit.

Tabla 13. Identificación y valoración de salvaguardas

SALVAGUARDAS			
Protección	**Tipo**	**Aplicación**	**Eficacia**
General	Autorizaciones previas	Activos, Equipos, redes, mantenimientos	L0
	Gestión de incidencias		L0
	Herramientas de seguridad		L0
Datos e información	Protección de la Información	Información y datos	L0
	Copias de seguridad de los datos (back up)		L0
	Aseguramiento de la integridad		L0

SALVAGUARDAS			
Protección	**Tipo**	**Aplicación**	**Eficacia**
	Cifrado de la información		L0
	Uso de firmas electrónicas		L0
	Uso de servicios de fechado electrónico (time stamping)		L0
Herramientas control de códigos amenaza	Actualizaciones de software controladas	Software, bases de datos, equipos	L0
	Actualizaciones controladas de Datos		L0
	Revisión de efectividad de programas		L0
Aplicaciones de carácter informático	Normatividad de uso de usuario	Normas de seguridad	L0
	Instalación solo de software autorizado con privilegios de administrador		L0
	Normatividad en copias de seguridad		L0
	Crear perfiles de seguridad		L0
	Control de versiones de software		L0
Equipos informáticos	Normatividad en uso de equipos	Equipos informáticos en general	L0
	Normatividad en procedimientos para el uso de equipos		L0
	Asignación de perfil de seguridad acorde a cargo		L0

SALVAGUARDAS			
Protección	**Tipo**	**Aplicación**	**Eficacia**
	Evitar todo acceso no autorizado a equipos por terceros		L0
	Seguridad en áreas de trabajo		L0
Seguridad en comunicaciones	Crear perfiles de seguridad	Comunicaciones acceso no autorizado	L0
	Verificar seguridad en servicios de red		L0
Soporte de información	Seguridad en contenedores de información	Información y datos	L0
	Protección criptográfica		L0
Instalaciones	Normatividad en centros y áreas	Equipos y ubicación de equipos	L0
	Especificaciones adecuadas para zonas informáticas		L0
	Vigilancia constante de equipos		L0

Fuente: El autor

Como se puede inferir del análisis de los datos consignados en la Tabla 13 (Identificación y valoración de salvaguardas) la institución se encuentra en una condición crítica y expuesta a la materialización de riesgos aprovechando las brechas de seguridad presentes pudiendo llegar a afectar la información y datos generados, manipulados y resguardados en la institución colegio PRO-COLOMBIANO.

Siendo así el desarrollo de este proyecto es fundamental en el propósito de proteger los activos de información presentes en la institución.

7.9. DETERMINACIÓN DEL RIESGO RESIDUAL

Se busca determinar si el impacto de la materialización de las amenazas disminuye con la aplicación de las salvaguardas identificadas en la institución colegio PRO-COLOMBIANO.

De acuerdo a los datos consignados y analizados en la Tabla 13 (Identificación y valoración de salvaguardas), se pudo determinar que la institución se encuentra en una situación incipiente de madurez en la protección de los activos de información propios de los procesos de matrículas y generación de calificaciones, lo que hace que realizar la determinación del riesgo residual sea una labor sin ningún sentido y que no genera valor agregado al desarrollo del proyecto, razón por la cual no se realizó esta actividad.

7.10. MANEJO Y TRATAMIENTO DE RIESGOS

En esta etapa del proyecto se busca determinar qué medidas se deben implementar en el colegio PRO-COLOMBIANO tendientes a remediar los problemas detectados y a gestionar la seguridad de ellos a lo largo del tiempo, con el propósito garantizar que las vulnerabilidades identificadas no continúen latentes, para de esta manera evitar que a futuro se puedan presentar nuevas vulnerabilidades que puedan convertirse en amenazas que pongan en riesgo los activos de información en la institución.

Es fundamental que las directivas del colegio PRO-COLOMBIANO tengan conocimiento de los tipos de manejo de riesgo que se pueden definir con el propósito de definir qué medidas de control o controles se pueden implementar para reducir, mitigar o en lo posible eliminar los posibles riesgos a los que está expuesta la institución, esto se puede ver en la Figura 11.

Figura 11. Tratamientos del riesgo en el SGSI

Fuente: Gestión y tratamiento de los riesgos, disponible en; https://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-9.pdf

En la Tabla 14 (Tipos de medidas de riesgo), se presentan las definiciones que contextualizan acerca de los tipos y medidas de manejo de riesgo que se pueden aplicar

Tabla 14. Tipos de medidas de riesgo

Medida	Descripción
Evitar el riesgo	Idealmente es la primera alternativa a efectuar, se logra evitando realizar las acciones que han tenido como resultado la materialización de riesgos a la seguridad de la información.
Reducir el riesgo	Cuando las acciones que se definan para evitar el riesgo no cumplen su cometido se requiere implementar acciones tendientes a reducir la probabilidad de ocurrencia y mitigar su impacto en el evento de su materialización. Se obtiene mediante la implementación de controles o el mejoramiento de los ya existentes.
Dispersar y atomizar el riesgo	Tomar acciones destinadas a distribuir el proceso que genera la materialización y la probabilidad de ocurrencia del riesgo a diferentes frentes, como ejemplo podemos citar el caso del almacenamiento de la información en un solo servidor, se recomienda definir procedimientos para back up de la información y almacenarla en diferentes sitios diferentes al de almacenaje principal, evitando concentración de la información confidencial en un solo sitio.
Transferir el riesgo	La organización debe buscar alternativas en terceros que le sirvan como apoyo para trasladar y compartir el riesgo y las consecuencias que conllevaría su materialización. Como ejemplo se puede citar la contratación de pólizas de seguros, la tercerización de procesos, entre otros.
Asumir el riesgo	Aceptar el riesgo residual después de aplicar los controles respectivos, para lo cual se deben definir planes de acción y constante monitoreo

Fuente: El autor

Teniendo definidos los parámetros para realizar el tratamiento de los posibles riesgos a los que se podría enfrentar colegio PRO-COLOMBIANO, en el Anexo G a este informe se presenta el mapa de riesgos donde se establecen las acciones recomendadas para manejarlos y evitar su materialización.

7.11. DECLARACIÓN DE APLICABILIDAD (SoA)

Habiendo identificado las brechas de seguridad de la información presentes en la institución educativa colegio PRO-COLOMBIANO y establecidas las medidas tendientes a la mitigación de los riesgos detectados y analizados, es indispensable que se desarrolle la declaración de aplicabilidad con los controles de seguridad a establecer que sirvan como una medida para contribuir a reforzar los procesos para protección de la información.

La declaración de aplicabilidad que se definió está basada en los controles de seguridad establecidos en el Anexo A del estándar ISO/IEC 27001 versión de 2013 donde se encuentra un conjunto de 14 dominios con 114 controles agrupados en 35 objetivos de control, con esta se pretende concretar los controles y los objetivos por los cuales se considera que estos son necesarios de implementar para afrontar las amenazas y vulnerabilidades identificadas con el fin de mitigar o aceptar los riesgos detectados y garantizar la protección de la información.

En el Anexo H se puede observar la declaración de aplicabilidad para la institución educativa colegio PRO-COLOMBIANO

8. MANUAL SGSI PARA COLEGIO PROCOLOMBIANO

Con la elaboración del manual se pretende que en la institución educativa colegio PRO-COLOMBIANO tengan definidos los lineamientos a seguir para la implementación de un sistema de seguridad de la información.

Se presenta un documento el cual está disponible en el Anexo I a este documento, el cual contiene el Manual de Gestión de seguridad de la información diseñado y propuesto para la institución, como resultado del análisis de las amenazas y vulnerabilidades identificadas en la institución y a la declaración de aplicabilidad (SoA) desarrollada.

9. DIVULGACIÓN

Para efectos de informar y concientizar a los empleados de la institución, sobre la definición e implementación de las normas, políticas y procedimientos que se definirán como resultado del desarrollo del proyecto de diseño de un SGSI para la institución, se sugiere:

- Realizar jornadas de capacitación sobre los temas que deben ser de conocimiento general de los empleados, y de los específicos de acuerdo a las funciones que desempeñe.
- Mantener disponible el manual SGSI diseñado para la institución (impreso y en medio magnético), para ser consultado por todo aquel que lo requiera de acuerdo a sus funciones.
- Realizar campañas de concientización sobre la importancia de atender los principios y lineamientos de seguridad de la información definidos para la institución los cuales son de obligatorio cumplimiento.
- Dar a conocer las sanciones disciplinarias y legales que acarrea para los empleados y la institución, el incumplimiento de las políticas, normas y procedimientos de seguridad de la información definidos para la institución.
- Contratar periódicamente los servicios de un especialista en Seguridad informática, que mantenga actualizados y vigentes los estándares y mejores prácticas en seguridad de la información, capacitando y actualizando al personal de la entidad.

CONCLUSIONES

Como resultado del análisis realizado a las medidas de protección de los activos de información de la institución educativa colegio PRO-COLOMBIANO, se identificaron las vulnerabilidades y amenazas que generan alto riesgo de fuga, pérdida o manipulación indebida de la información, por lo que se requiere con urgencia la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en dicha institución.

Lo anterior en razón a que se estableció que en la institución no se tienen definidas normas, políticas y procedimientos tendientes a proteger los activos de información de los procesos de matrículas y calificaciones de los alumnos de la institución, lo que genera alto riesgo de pérdida de información, posibles demandas de los afectados y sanciones de tipo administrativo por parte de los entes de control.

Las directivas de la institución al tomar la decisión de implementar el SGSI diseñado en este proyecto cumplirían los objetivos de afianzar su compromiso en el sentido de proteger sus activos de información al tomar conciencia de la importancia de que se diseñen, definan y establezcan medidas tendientes a evitar la materialización de riesgos que afecten la seguridad de la información, mitigando el impacto que estos puedan ocasionar en la institución.

BIBLIOGRAFÍA

[1] Alcaldía de Bogotá. Ley 1273 de 2009 consulta de la norma. Internet:(http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492).

[2] _____. Constitución política de Colombia. Internet:(http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4125).

[3] _____. Ley 527 del 18 de Agosto de 1999. Internet: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276).

[4] _____. Ley 1266 de 2008. Internet: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488)

[5] _____. Ley 1581 de 2012. Internet: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981).

[6] _____. Decreto 1377 del 27 de junio de 2013. Internet: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646)

[7] BALDECCHI, Rodrigo. Implementación efectiva de un SGSI ISO 27001. Internet: (http://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014%20-%20Exposici%C3%B3n%202%20CIGRAS%20ISO%2027001%20-%20rbq.pdf)

[8] Certicamara. ColombiaDigital, ABC para proteger los datos personales, Ley 1581 de 2012 Decreto 1377 de 2013. Internet: (https://www.colombiadigital.net/actualidad/articulos-informativos/item/5543-abc-para-proteger-los-datos-personales-ley-1581-de-2012-decreto-1377-de-2013.html).

[9] Colegio PRO-COLOMBIANO. Proyecto educativo institucional (PEI). 2003, 89p.

[10] COLOMBIA. MINISTERIO DE EDUCACIÓN NACIONAL. Ley general de educación de 1994. Internet: (http://www.mineducacion.gov.co/1759/articles-124745_archivo_pdf9.pdf).

[11] _____. “Decreto 1290”. Internet: (http://www.mineducacion.gov.co/1621/articles-187765_archivo_pdf_decreto_1290.pdf)

[12] _____. “Decreto 1860”. Internet: (http://www.mineducacion.gov.co/1621/articles-172061_archivo_pdf_decreto1860_94.pdf)

[13] CÓRDOVA, Cesar, MORALES, Gustavo, SANAMÉ, José. Desarrollo de un SGSI para los colegios profesionales en la región Lambayeque. Caso de estudio: Colegio de ingenieros. Internet: (https://issuu.com/gustavomorales02/docs/art__culo_cient__fico_cip_25-02-201/1)

[14] DÍAZ, Andrés, COLLAZOS Gloria, LOZANO Hermes, ORTIZ Leidy, HERAZO Gustavo. Implementación de un sistema de gestión de seguridad de la información (SGSI) en la comunidad nuestra señora de gracia, alineado tecnológicamente con la norma ISO 27001. Universidad Konrad Lorenz. Internet: http://www.konradlorenz.edu.co/images/stories/articulos/SGSI.pdf

[15] Educación. Universidades que están en la norma 27001 certificada. Internet: (http://es.educationcollege.info/college-higher-education/college/1008025022.html)

[16] GTC-ISO/IEC 27003:2012, Tecnología de la información. técnicas de seguridad. Guía de implementación de un sistema de gestión de la seguridad de la información.

[17] ISO 27000.es. El portal de ISO 27001 en Español. Internet:(http://www.iso27000.es/sgsi.html).

[18] JUÁREZ, Héctor. ISO 27001, para qué es y para qué sirve (parte 1), Magazcitum, magazine para los profesionales de la seguridad de TI. Internet: (http://www.magazcitum.com.mx/?p=1574#.WFB7Ri_QBjq).

[19] LEASING BOLIVAR. Manual del Sistema de Gestión de Seguridad de la Información.

[20] NTC-ISO/IEC 27001:2013. Information Technology. Security Techniques. Information Security Management Systems. Requirements.

[21] Policía Nacional de Colombia, Resolución 03049 del 24 de agosto de 2012, “Por la cual se adopta el manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional”. Internet: (http://www.policia.edu.co/documentos/normatividad_2016/manuales/Manual%20del%20sistema%20de%20gesti%C3%B3n%20de%20seguridad%20de%20la%20informaci%C3%B3n%20para%20la%20Polic%C3%ADa%20Nacional.pdf)

[22] SALCEDO, Robín. Plan de implementación del SGSI basado en la NORMA ISO 27001:2013, resumen ejecutivo memoria TFM plan de implementación del SGSI. Internet: (http://openaccess.uoc.edu/webapps/o2/bitstream/10609/41002/4/rsalcedobTFC1214memoria.pdf).

[23] Universidad del Atlántico. Sistema de gestión de seguridad de la información, Normatividad vigente. Internet: (http://www.uniatlantico.edu.co/uatlantico/administrativa/SGSI%20-%20Normatividad).

[24] Universidad Nacional Autónoma de México. Fundamentos de seguridad informática, definiciones. Internet: (http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/Definiciones.php).

[25] Universidad Nacional Abierta y a Distancia – UNAD. Datateca curso SGSI. Capítulo 5.1.1 Fase 1: Planificar: Análisis diferencial para definición del alcance y otras. Internet: (http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/511_fase_1_planificar_anlisis_diferencial_para_definicin_del_alcance_y_otras_actividades_de_planeacin.html).

ANEXOS

Anexo A. Carta de Aval del proyecto expedida por el colegio PRO-COLOMBIANO

COLEGIO PRO-COLOMBIANO
AFIANZANDO VALORES Y DERECHOS HUMANOS

Cra 19 No. 56 - 81 Sur San Carlos
Bogotá D.C.
colegioprocolombiano@gmail.com
FIRMA REGISTRADA NOTARIA 57

COLEGIO PRO-COLOMBIANO
JUSTICIA
LIBERTAD
SABIDURIA
EDUCACION MIXTA

RESOLUCIÓN 5964 DE 07/94 S.E
INSCRIPCIÓN S.E. 2560
INSCRIPCIÓN DANE 211001026497
Tel 7697655 Bogotá

Bogotá, marzo 15 de 2016

Ingeniero
Jerzon Álvarez Riaño
Ciudad

Referencia: Aceptación propuesta de implementación SGSI

Respetuoso saludo,

Atentamente me permito comunicarle que las directivas de nuestro Colegio, analizaron y aprobaron la propuesta presentada por usted, para diseñar un sistema de gestión de seguridad de la información - SGSI, que incluye la respectiva asesoría y planeación para su implementación.

Por lo anterior, le autorizamos el acceso a la información necesaria para desarrollar dicha propuesta y estaremos prestos a atender sus requerimientos.

Como es de su conocimiento, la información a la que usted tendrá acceso es estrictamente confidencial, por lo que no puede ser divulgada a terceros no autorizados por el Colegio.

Quedamos atentos a cualquier inquietud.

Atentamente,

Rosa Edelmira Salazar Salamanca
Rectora – Propietaria

-COLEGIO PRO-COLOMBIANO TL. 7697655 BOGOTÁ-

Anexo B. Acta de aceptación del proyecto y conformación comité SGSI

COLEGIO PRO-COLOMBIANO

APIANZANDO VALORES Y DERECHOS HUMANOS

Cra 19 No. 56 - 81 Sur San Carlos
Bogotá D.C.
colegioprocolombiano@gmail.com
FIRMA REGISTRADA NOTARIA 57

RESOLUCIÓN 5964 DE DIC/94 S.E
INSCRIPCIÓN S.E. 2560
INSCRIPCIÓN DANE 31100126497
Tel 7697655 Bogotá

ACTA DE FORMALIZACIÓN DEL PROYECTO

Código:	**COL_PROCOL_SGSI-001**
Versión:	**0.1**
Fecha de la versión:	**19/09/2016**
Creado por:	Ing. Jerzon Álvarez
Aprobado por:	Lic. Rosa Edelmira Salazar
Nombre del archivo:	SGSI-001 – Acta de constitución del Proyecto.docx
Nivel de confidencialidad:	Media

Asistentes

Nombre	Cargo	Asistió (SI/NO)
Licenciada Rosa Edelmira Salazar	Rectora propietaria Colegio PRO-COLOMBIANO	SI
Licenciado Hernando Vergara	Profesor de sistemas Colegio PRO-COLOMBIANO	SI
Licenciada Rosario Valero	Coordinadora Colegio PRO-COLOMBIANO	SI
Ingeniero Jerzon Herley Álvarez	Project Manager proyecto	SI

El día 19 de septiembre de los corrientes, se realizó la reunión preliminar con las directivas del Colegio PRO-COLOMBIANO en sus instalaciones, con el objetivo de desarrollar los siguientes temas:

1. Presentar el plan de trabajo que se desarrollará durante la ejecución del proyecto e identificar las dependencias donde se pueden identificar los activos de información de la institución.
2. Conformar el comité de Sistema de Gestión de Seguridad de la Información, en adelante SGSI con el fin de obtener su autorización en cada una de las actividades definidas en el plan de trabajo descritos.

-COLEGIO PRO-COLOMBIANO TL. 7697655 BOGOTÁ-

COLEGIO PRO-COLOMBIANO

APIANZANDO VALORES Y DERECHOS HUMANOS

Cra 19 No. 56 - 81 Sur San Carlos
Bogotá D.C.
colegioprocolombiano@gmail.com
FIRMA REGISTRADA NOTARIA 57

RESOLUCIÓN 5964 DE DIC/94 S.E
INSCRIPCIÓN S.E. 2560
INSCRIPCIÓN DANE 31100126497
Tel 7697655 Bogotá

Historial de Revisiones

Fecha	Versión	Modificado/Creado por	Descripción de la modificación
19/09/2016	0.1	Ing. Jerzon Álvarez	Creación del primer documento

Aprobación

Fecha	Nombre	Cargo	Firma
19/09/2016	Lic. Rosa Edelmira Salazar	Rectora – propietaria Colegio PRO-COLOMBIANO	Firmado el original

Mejora Continua

Fecha	Revisor/Auditor	Resumen Observaciones

COLEGIO PRO-COLOMBIANO

Afianzando Valores y Derechos Humanos

Cra 19 No. 56 - 81 Sur San Carlos
Bogotá D.C.
colegioprocolombiano@gmail.com
FIRMA REGISTRADA NOTARIA 57

RESOLUCIÓN 5964 DE DIC/94 S.E
INSCRIPCIÓN S.E. 2560
INSCRIPCIÓN DANE 311001126497
Tel 7697655 Bogotá

Nombre del Proyecto	**Siglas del Proyecto**
DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI BASADO EN LA NORMA ISO27001 PARA EL COLEGIO PRO-COLOMBIANO DE LA CIUDAD DE BOGOTÁ, QUE INCLUYE: ASESORÍA, PLANEACIÓN.	SGSI-001
Descripción del Proyecto: *Qué, quién, cómo, cuándo y dónde?*	
La implementación del SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI BASADO EN LA NORMA ISO27001, será desarrollado por el ingeniero Jerzon Álvarez, mediante la identificación de las vulnerabilidades a las que están expuestas los activos de información generados en los procesos de matrículas y calificaciones de la institución, para garantizar que los riesgos de la seguridad de la información se evalúan, asumen, gestionan, controlan y monitorean a fin de minimizar su materialización, implementando políticas, normas y procedimientos que aseguren la información adecuadamente. El proyecto se desarrollará entre el 19 de septiembre al 11 de diciembre de 2016, en el Colegio PRO-COLOMBIANO de la ciudad de Bogotá.	
Definición del Producto del Proyecto: *Descripción del producto a generar.*	
El desarrollo del proyecto permitirá garantizar la integridad, confidencialidad y disponibilidad de la información en custodia del colegio PRO-COLOMBIANO que es generada en los procesos de matrícula y calificaciones, en pro del cumpliendo de los objetivos estratégicos de la institución.	
Definición de Requisitos del Proyecto	
Como resultado de este proyecto se entregara un manual con el SGSI a implementar en la institución educativa colegio PRO-COLOMBIANO.	

Objetivos del Proyecto: *Metas establecidas del proyecto*		
Concepto	***Objetivos***	***criterio de Éxito***
1. Alcance	El alcance definido para la implementación del sistema de gestión de seguridad de la información en la institución educativa colegio PRO-COLOMBIANO está enfocado a los procesos de matrícula y procesamiento de las calificaciones de los alumnos de la institución	Aprobación de todos los entregables al cliente
2. Tiempo	El proyecto debe terminarse dentro del plazo acordado.	Finalizar el proyecto en un plazo de 82 días calendario a partir del 19 de Septiembre de 2016
3. Costo	El presupuesto del proyecto es de $3.894.000	No exceder el presupuesto calculado.

Cra 19 No. 56 - 81 Sur San Carlos
Bogotá D.C.
colegioprocolombiano@gmail.com
FIRMA REGISTRADA NOTARIA 57

RESOLUCIÓN 5964 DE DIC/94 S.E
INSCRIPCIÓN S.E. 2560
INSCRIPCIÓN DANE 31100126497
Tel 7697655 Bogotá

DESIGNACIÓN DEL PROJECT MANAGER DEL PROYECTO.		
NOMBRE	Ing. Jerzon Álvarez	*NIVELES DE AUTORIDAD*
REPORTA A	Rectora – Propietaria	Aprueba el SGSI
SUPERVISA A	Comité SGSI	

CRONOGRAMA DEL PROYECTO.				
ACTIVIDADES (TAREAS)			*FECHA PROGRAMADA*	
DESCRIPCIÓN TAREAS	FECHA INICIO	DURACIÓN EN DÍAS	FECHA FINAL	RESPONSABLES
Determinar el alcance y objetivos del SGSI	19/09/2016	3	22/09/2016	Jerzon Álvarez, directivas de la Institución
Identificación de los activos de información	23/09/2016	15	08/10/2016	Personal de la Institucional, acompañamiento del comité
Identificación de amenazas y vulnerabilidades	09/10/2016	15	24/10/2016	Jerzon Álvarez
Identificar los impactos	25/10/2016	15	09/11/2016	Jerzon Álvarez
Análisis y evaluación del riesgo	10/11/2016	15	25/11/2016	Jerzon Álvarez
Selección de controles y SOA, y elaboración del manual	26/11/2016	15	11/12/2016	Jerzon Álvarez, directivas de la Institución

DEFINICIÓN DE INTEGRANTES QUE INTERVIENEN EN EL PROYECTO. (COMITÉ SGSI)	
ROL	*FUNCIONES*
Representante legal (Licenciado Rosa Edelmira Salazar)	Responsable de ejercer control, seguimiento, revisión y supervisión de las tareas propias del proyecto.
USUARIO DE SERVICIOS DE INFORMACIÓN (Licenciada Rosario Valero)	Responsable de la información, activo o servicio informático quien apoyará al especialista de Seguridad de la Información suministrando la información que este requiera para la ejecución del proyecto, adicionalmente apoyará en la definición de conceptos y políticas a implementar.
ADMINISTRADOR DE SEGURIDAD INFORMÁTICA (Licenciado Hernando Vergara)	Persona con conocimientos especializados informática, quien apoyara el desarrollo de las actividades de evaluación de los sistemas y servicios informáticos y de telecomunicaciones presentes en la institución, adicionalmente apoyará en la definición de conceptos y políticas a implementar.
ESPECIALISTA DE SEGURIDAD DE LA INFORMACIÓN (Ingeniero Jerzon Álvarez)	Experto en Seguridad informática quien se encarga del desarrollo de las actividades de planeación, evaluación del modelo de seguridad de la información y asesoría para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en la institución.

Cra 19 No. 56 - 81 Sur San Carlos
Bogotá D.C.
colegioprocolombiano@gmail.com
FIRMA REGISTRADA NOTARIA 57

RESOLUCIÓN 5964 DE DIC/94 S.E
INSCRIPCIÓN S.E. 2560
INSCRIPCIÓN DANE 31100126497
Tel 7697655 Bogotá

AMENAZAS DEL PROYECTO
• Poco compromiso del equipo asignado al proyecto. • Falta de colaboración por parte de los funcionarios para la entrega de información • Ausencia de recursos asignados al proyecto. • Cambio de las fechas definidas en el cronograma para la entrega de avances y producto final. • Cambio de los integrantes del comité SGSI. • Definición de excesivos controles.

PRESUPUESTO PRELIMINAR DEL PROYECTO.

Recurso utilizado	Cantidad	Responsable	Descripción	Valor unitario	Valor presupuestado
Materiales	2	Colegio PRO-COLOMBIANO	Resma de papel tamaño carta	$12.000	$ 24.000
Físicos	82 días	Colegio PRO-COLOMBIANO	Instalaciones del colegio PRO-COLOMBIANO, asignación de oficina para ejecución de labores propias del proyecto, incluido suministro de servicios de luz e Internet.	$10.000	$820.000
Humano	1	Colegio PRO-COLOMBIANO	Funcionario apoyo labores levantamiento de información (15 días), funciones adicionales asignadas.	$400.000	$400.000
	40 días	Ing. Jerzon Álvarez	Transporte, alimentación	$20.000	$800.000
Tecnológicos	1	Colegio PRO-COLOMBIANO	Computador portátil	$1.000.000	$1.000.000

COLEGIO PRO-COLOMBIANO

APIANZANDO VALORES Y DERECHOS HUMANOS

Cra 19 No. 56 - 81 Sur San Carlos
Bogotá D.C.
colegioprocolombiano@gmail.com
FIRMA REGISTRADA NOTARIA 57

RESOLUCIÓN 5964 DE DIC/94 S.E
INSCRIPCIÓN S.E. 2560
INSCRIPCIÓN DANE 311001126497
Tel 7697655 Bogotá

PRESUPUESTO PRELIMINAR DEL PROYECTO.					
Recurso utilizado	Cantidad	Responsable	Descripción	Valor unitario	Valor presupuestado
	1	Colegio PRO-COLOMBIANO	Disco duro portátil	$250.000	$250.000
	1	Colegio PRO-COLOMBIANO	Impresora	$200.000	$200.000
	1	Colegio PRO-COLOMBIANO	Video beam	$400.000	$400.000
Total					$3.894.000

PROMOTOR QUE AUTORIZA EL PROYECTO.			
NOMBRE	*EMPRESA*	*CARGO*	*FECHA*
ROSA EDELMIRA SALAZAR	Colegio PRO-COLOMBIANO	Rectora Propietaria	19/09/2016

ROSA EDELMIRA SALAZAR SALAMANCA
Rectora - Propietaria

ANEXO C. FORMULARIO DE INSCRIPCIÓN COLEGIO PRO-COLOMBIANO

FORMULARIO DE INSCRIPCIÓN AÑO _____
COLEGIO PRO-COLOMBIANO
RESOLUCIÓN DE APROBACIÓN OFICIAL N°5964 DE 1994
"Afianzando Valores y Derechos Humanos"
Resolución de Aprobación No 5964 de Dic/94 S.E.D
Primaria completa
Sede Cra. 19 No 56 – 81 sur San Carlos
Numero Tel: 769 76 55

INFORMACIÓN REQUERIDA DEL ESTUDIANTE

Nombre del Aspirante: _____
Curso para el cual solicita cupo: _____
Fecha y lugar de nacimiento del aspirante: _____
Edad: _____. Documento de identidad: _____
¿Existe algún tipo de condición de salud de la cual EL COLEGIO debería estar al tanto? _____
_____
Motivos de cambio de Colegio: _____
_____

INFORMACIÓN ACADÉMICA

Relacionar las tres últimas instituciones educativas, el año, el grado que cursó en ellas y el carácter de la institución.

AÑO	GRADO	NOMBRE DEL COLEGIO	CARÁCTER	
			OFICIAL	PRIVADO

CONCEPTO DE CONVIVENCIA

BREVE DESCRIPCIÓN DEL ESTUDIANTE EN SU ENTORNO ESCOLAR

_____
_____

COMPORTAMIENTO Y DISCIPLINA: S ____ A: ____ B: ____ BJ: ____
SEGUIMIENTO DE NORMAS: S ____ A: ____ B: ____ BJ: ____
RELACIÓN COM SUS COMPAÑEROS Y DOCENTES: S ____ A: ____ B: ____ BJ: ____

INFORMACIÓN ACUDIENTES DEL ESTUDIANTE

Nombre del padre: _____ Ocupación: _____
Dirección: _____ Teléfono fijo: _____
Teléfono celular: _____ Email: _____

Nombre de la madre: _____ Ocupación: _____
Dirección: _____ Teléfono fijo: _____
Teléfono celular: _____ Email: _____

Nombre del acudiente: _____ Ocupación: _____
Dirección: _____ Teléfono fijo: _____
Teléfono celular: _____ Email: _____

COMPROMISO FAMILIAR

	ASPECTO	S	A	B	BJ
1	Compromiso de los padres frente al proceso de formación de su hijo.				
2	Asistencia y participación de los padres en actividades institucionales.				
3	Asistencia y cumplimiento a reuniones o citaciones.				
4	Respeto para presentar inconformidades o desacuerdos.				
5	Puntualidad en el pago de compromisos económicos con el colegio.				

Nota: la adquisición del formulario no implica ninguna vinculación directa con la institución hasta no formalizar la matrícula en la secretaría. Tampoco guardar el cupo por tiempo indefinido sino se formalizó la matrícula dentro de los tiempos establecidos.
Consejo Directivo

ANEXO D. FORMATO HOJA DE MATRICULA COLEGIO PRO-COLOMBIANO

COLEGIO PRO-COLOMBIANO

APROBACION OFI. 5964 DIC/1994 S.E.

"AFIANZANDO VALORES Y DERECHOS HUMANOS"

TELÉFONO 7697655

Matricula Nº_____ Renovación_____ Folio Nº_____

Fecha: _____

Apellidos y nombres _____

Documento: _____ No.:_____De_____

Nacido en: _____el:_____Edad_____

Inicia el Grado: _____

Cursó el grado inmediatamente anterior en el plantel Educativo_____

_____

Presenta: Boletín_____ Registro_____Fotos_____Vacunas_____EPS_____

Nombre del padre: _____

Nombre de la madre: _____

Dirección: _____ Teléfono_____

Acudiente: _____ Parentesco _____

Dirección: _____Teléfono_____

Observaciones_____

_____

Nos comprometemos a conocer y participar de los ajustes del P.E.I. y Vivenciar el Pacto de convivencia

_____ _____

PADRE DE FAMILIA O ACUDIENTE ESTUDIANTE

_____ _____

RECTORA SECRETARIO

ANEXO E. FORMATO INFORME ACADÉMICO COLEGIO PRO-COLOMBIANO

COLEGIO PRO-COLOMBIANO

EDUCACIÓN MIXTA
APROBACIÓN OFICIAL No 5964 DE 1994
"Afianzando Valores y Derechos Humanos"

ESTUDIANTE:		
GRADO:	AÑO:	PERIODO ACADÉMICO:

ÁREA	COMPETENCIAS Y DESEMPEÑOS	NOTA	FALLAS	I.H.S.
MATEMÁTICAS 				4
HUMANIDADES LENGUA CASTELLANA 				4
CIENCIAS NATURALES Y EDUCACIÓN AMBIENTAL 				4
CIENCIAS SOCIALES, CONSTITUCIÓN POLÍTICA Y DEMOCRÁTICA 				4

ÁREA	COMPETENCIAS Y DESEMPEÑOS	NOTA	FALLAS	I.H.S.
EDUCACIÓN FÍSICA RECREACIÓN Y DEPORTES 				2
EDUCACION RELIGIOSA 				2
EDUCACION ARTÍSTICA MÚSICA Y DANZAS 				2
EDUCACION ETICA Y VALORES 				2
TECNOLOGÍA E INFORMÁTICA 				2
HUMANIDADES LENGUA EXTRANJERA INGLÉS 				3
COMPORTAMIENTO ESCOLAR 				
CONTABILIDAD Y EMPRENDIMIENTO 				2

ESCALA CONCEPTUAL	S:Desempeño Superior = 5 A 4,5	A: Desempeño Alto= 4,4 A 3,5
	B:Desempeño Básico = 3,4 A 3,0	Bj: Desempeño Bajo= Menor a 3.0
ESTE DOCUMENTO ES VALIDO CON FIRMA Y SELLO DE RECTORÍA		

OBSERVACIONES GENERALES

PROFESOR: _____ RECTORA: _____

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX LIC. ROSA EDELMIRA SALAZAR SALAMANCA

"El que cambia en el alma de un niño cambia para siempre" Anónimo

ANEXO F. FORMATO SABANA DE NOTAS COLEGIO PRO-COLOMBIANO

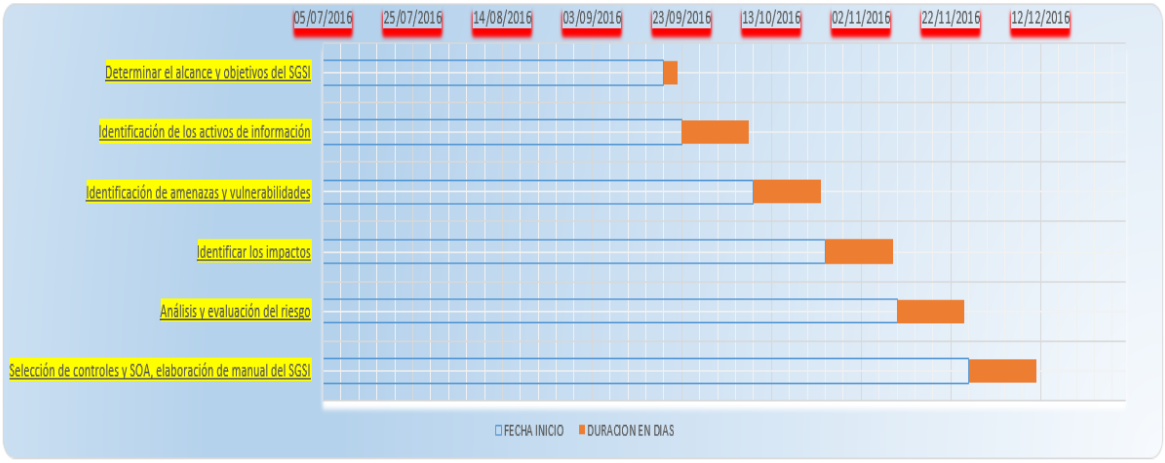
COLEGIO PRO-COLOMBIANO
EDUCACIÓN MIXTA. APROBACIÓN OFICIAL N°5964 DE 1994
"Afianzando Valores y Derechos Humanos"
DIRECTOR DE GRADO: _____ SÁBANA DE NOTAS PERIODO ACADÉMICO: _____

N	ESTUDIANTE	MATEMÁT	LENGUAJE	C. NATURALES	C. SOCIALES	EDU FÍSICA	RELIGIÓN	ARTÍSTI	ÉTICA	CONTAB	INFORM	INGLES
1												
2												
3												
4												
5												
6												
7												
8												
9												
10												
11												
12												
13												
14												
15												
16												
17												
18												
19												
20												
21												
22												
23												
24												
25												
26												
27												
28												
29												
30												

ESCALA CONCEPTUAL
S: Superior (4,5 a 5,0); A: Alto (4,4 a 3,5); B: Básico (3,4 a 3,0); Bj: Bajo (<3).

ANEXO G. CRONOGRAMA DE ACTIVIDADES DEL PROYECTO

TAREA	DESCRIPCIÓN TAREAS	FECHA INICIO	DURACION EN DIAS	FECHA DE FIN	RESPONSABLES
1	Determinar el alcance y objetivos del SGSI	19/09/2016	3	22/09/2016	Jerzon Alvarez Riaño, directivas de la institución
2	Identificación de los activos de información	23/09/2016	15	08/10/2016	Personal de la institución, acompañamiento del comité
3	Identificación de amenazas y vulnerabilidades	09/10/2016	15	24/10/2016	Jerzon Alvarez Riaño
4	Identificar los impactos	25/10/2016	15	09/11/2016	Jerzon Alvarez Riaño
5	Análisis y evaluación del riesgo	10/11/2016	15	25/11/2016	Jerzon Alvarez Riaño
6	Selección de controles y SOA, elaboración de manual del S	26/11/2016	15	11/12/2016	Jerzon Alvarez Riaño, directivas de la institución



ANEXO H. MAPA DE RIESGOS PROBABLES

ACTIVO	AMENAZAS	RIESGOS ASOCIADOS	CAUSAS	CONSECUENCIAS	RECOMENDACIONES		CONTROLES ASOCIADOS
					ACCIONES A SEGUIR	MONITOREO	
INFORMACIÓN	Hurto o robo (información, documentos, medios o equipos).	Perdida de información	Falta de Políticas de Seguridad	Retrasos en la realización de las actividades.	Mitigar, mediante la implementación de controles, buscando que la probabilidad de ocurrencia disminuya.	Establecer planillas donde se registre quien genera, modifique la información.	Pruebas de seguridad de sistemas
	Divulgación no autorizada	Ataques informáticos	Ataques intencionados	Perdidas económicas			Registro y análisis de eventos
	Daño accidental (incendio, agua, humedad, contaminación química, construcción, entre otros)	Demandas penales por parte de los usuarios	Agujeros de seguridad en los sistemas operativos.	Pérdida de clientes	Realizar backups	Establecer planillas para uso de información confidencial.	Control de acceso a códigos fuente de programas
	Ataques maliciosos (vandalismo, hurto,).	Sanciones administrativas por parte de la secretaria de educación	Agujeros de seguridad en las aplicaciones.	Perdida reputacional.			
	Uso no autorizado de recursos (equipos de comunicación, medios de almacenamiento, sistemas de información.	Sanciones administrativas por parte del Ministerio de educación	Errores en las configuraciones de los sistemas.	Demandas penales por uso indebido de información confidencial.	Evitar, identificando y evitando las causas propendiendo por su no materialización.	Instalar cámaras de vigilancia en sala de informática y archivo.	Respaldo de la información
	Acceso no autorizado a la información o a las instalaciones (oficinas, edificio, sala, centro de cómputo, etc.)	Generación de certificados de estudio falsos.	Usuarios carentes de información respecto al tema	Perdida de la personería jurídica y cierre de la institución	Cifrado de información e implementación de firmas digitales		Política sobre el uso de controles criptográficos
	Intrusión o acceso forzado (instalaciones, sistemas de información, información).		No existen backups				Restricción de acceso a la información
							Política sobre el uso de

ACTIVO	AMENAZAS	RIESGOS ASOCIADOS	CAUSAS	CONSECUENCIAS	RECOMENDACIONES		CONTROLES ASOCIADOS
					ACCIONES A SEGUIR	MONITOREO	
	Incumplimiento de políticas o procedimientos internos.		No existe control de acceso al archivo de la institución.		Dispersar y atomizar el riesgo, creando backups de la información		controles criptográficos ISO 27001: 2013 Dominio 5 Políticas de seguridad ISO 27001: 2013 Dominio 8 Gestión de activos ISO 27001: 2013 Dominio 9 Control de accesos ISO 27001: 2013 Dominio 10 Cifrado
	Código malicioso (troyanos, gusanos, virus, entre otros)						
SOFTWARE	Código malicioso (troyanos, gusanos, bomba lógica, entre otros).	Ataques informáticos Degradación de información	Agujeros de seguridad en los sistemas operativos. Agujeros de seguridad en las aplicaciones.	Retrasos en la realización de las actividades. Pérdida o degradación de información.	Mitigar, mediante la implementación de controles, buscando que la probabilidad de ocurrencia disminuya.	Pruebas de seguridad de sistemas Registro y análisis de eventos	Pruebas de seguridad de sistemas Registro y análisis de eventos.
	Falla o mal funcionamiento del Software						

ACTIVO	AMENAZAS	RIESGOS ASOCIADOS	CAUSAS	CONSECUENCIAS	RECOMENDACIONES		CONTROLES ASOCIADOS
					ACCIONES A SEGUIR	MONITOREO	
	Errores de transmisión o almacenamiento.	Interrupciones en los procesos	Errores en las configuraciones de los sistemas.		Actualización de paquetes informáticos y de protección antivirus a las últimas versiones disponibles.		Políticas sobre uso de contraseñas seguras para acceso a los aplicativos.
	Ataques contra el sistema, manipulación de software, manipulación de equipo informático, entre otros).	Manipulación de información	Usuarios carentes de información respecto al tema				ISO 27001: 2013 Dominio 9 gestión de accesos
	Uso de software no licenciado o no autorizado.		Licencias vencidas o a punto de expirar.		Incentivar uso de contraseñas a los aplicativos		ISO 27001: 2013 Dominio 14.2 seguridad en los procesos de desarrollo y soporte
			No hay políticas sobre uso de contraseñas				
HARDWARE	Falla o mal funcionamiento del hardware.	Interrupciones en los procesos	Falta de mantenimiento	Retrasos en la realización de las actividades.	Mitigar, mediante la implementación de controles, buscando que la probabilidad de ocurrencia disminuya.	Planillas uso de equipos.	Procedimientos de operación documentados
	Avería de origen físico o lógico.	Perdida de información	Equipos obsoletos				Políticas sobre uso de equipos
	Perdida de equipos		No existe inventario actualizado de equipos.				ISO 27001: 9.2.4 Mantenimiento de equipos.

ACTIVO	AMENAZAS	RIESGOS ASOCIADOS	CAUSAS	CONSECUENCIAS	RECOMENDACIONES		CONTROLES ASOCIADOS
					ACCIONES A SEGUIR	MONITOREO	
SOPORTES DE INFORMACIÓN	Intrusión o acceso forzado (instalaciones, sistemas de información, información). Hurto o robo (información, documentos, medios o equipos). Divulgación no autorizada. Incumplimiento de políticas o procedimientos internos. Daño accidental (incendio, agua, humedad, contaminación química, construcción, entre otros)	Interrupciones en los procesos Manipulación de información Perdida de información	No existe responsable definido No existen back-ups No existen políticas para manipulación y resguardo de soportes de información No existe inventario de soportes de información y de su contenido	Perdida de información	Mitigar, mediante la implementación de controles, buscando que la probabilidad de ocurrencia disminuya. Realizar back-ups de la información creando discos duros virtuales.	Establecer planillas donde se registre responsable de los soportes de información, fechas de actualización de información registrando el tipo y el responsable de la actualización	Definir responsables Realizar back-ups de la información Verificar estado de los soportes de información mediante el uso de software antivirus ISO 27001: 11.2 Seguridad de los equipos
REDES DE TELECOMUNICACIONES	Falla o mal funcionamiento Avería de origen físico o lógico. Perdida de equipos	Interrupciones en los procesos Retrasos en la ejecución de los procesos de reporte	Daño en la red del proveedor Falta de pago del servicio	Retrasos en la realización de las actividades. Sanciones administrativas debido al no reporte obligatorio de	Mitigar, mediante la implementación de controles, buscando que la probabilidad de ocurrencia disminuya.	Llevar planillas donde se registre fechas de pago del servicio.	ISO 27001: 2013 Dominio 14.1 Requisitos de seguridad de los sistemas de información

ACTIVO	AMENAZAS	RIESGOS ASOCIADOS	CAUSAS	CONSECUENCIAS	RECOMENDACIONES		CONTROLES ASOCIADOS
					ACCIONES A SEGUIR	MONITOREO	
	Falla sistema de comunicaciones (Internet).	al ministerio de educación.		novedades al ministerio de educación			
EQUIPAMENTO AUXILIAR	Falla o mal funcionamiento Avería Falta de mantenimientos preventivos	Interrupciones en los procesos Retrasos en la ejecución de los procesos	Falta de mantenimiento preventivo. No hay responsables definidos para la administración del equipamiento No se ha realizado capacitación al personal al respecto No existe equipo de respaldo de energía comercial (UPS)	Daño de información. Perdida de información Retrasos en la realización de las actividades. Perdidas económicas	Mitigar, mediante la implementación de controles, buscando que la probabilidad de ocurrencia disminuya. Contratar back-up para proveedor de servicio de Internet	Llevar planillas de control y registro de mantenimientos preventivos	Mantenimiento periódico de equipos
PERSONAS	Intruso externo (Ej. exempleado, delincuente informático, interesados. Empleados (acciones involuntarias y/o deliberadas).	Interrupciones en los procesos Retrasos en la ejecución de los procesos.	Ausencia de monitoreo de ejecución de procesos	Daño de información. Perdida de información	Mitigar, mediante la implementación de controles, buscando que la probabilidad de ocurrencia disminuya.	Planillas control de acceso al archivo. Planillas para recibo de información,	Acuerdos y cláusulas de confidencialidad para el personal con acceso a información sensible

ACTIVO	AMENAZAS	RIESGOS ASOCIADOS	CAUSAS	CONSECUENCIAS	RECOMENDACIONES		CONTROLES ASOCIADOS
					ACCIONES A SEGUIR	MONITOREO	
	Proveedor o contratista.		Personal inconforme Ingeniería social No se han realizado capacitaciones en tema de seguridad informática.	Retrasos en la realización de las actividades. Perdidas económicas	Programar jornadas de capacitación sobre el tema de seguridad de la información	definiendo responsables y el tipo de información entregada.	Jornadas de capacitación Revisar periódicamente las carpetas de los empleados a fin de tener certeza de que han firmado los documentos de entrega de reportes de notas. Establecer procedimientos para manejo de información sensible. ISO 27001: 2013 Dominio 7 Seguridad ligada a los recursos humanos
	Uso no autorizado de recursos (equipos de comunicación, medios de almacenamiento, sistemas de información, computadores.						
	Manipulación del sistema.						
	Espionaje (ingeniería social).						
	Abuso de derechos (de usuario, de administrador).						
	Acceso no autorizado a la información o a las instalaciones (oficinas, edificios, archivo, sala de cómputo,						
	Intrusión o acceso forzado (instalaciones, sistemas de información, información).						
	Hurto o robo (información, documentos, medios o equipos)						

ACTIVO	AMENAZAS	RIESGOS ASOCIADOS	CAUSAS	CONSECUENCIAS	RECOMENDACIONES		CONTROLES ASOCIADOS
					ACCIONES A SEGUIR	MONITOREO	
	Error en el uso (de equipos, medios, información, sistemas o servicios de información).						
INFRAESTRUCTURA	Ataque malicioso (terrorismo, vandalismo, hurto). Desastre natural (temblor, terremoto, inundación, incendio,). Daño accidental (incendio, agua, humedad).	Interrupciones en los procesos Retrasos en la ejecución de los procesos Para total de las actividades	Catástrofes naturales No existe seguro contra catástrofes No hay sistema de vigilancia (cámaras de seguridad)	Para en la operación Pérdida de clientes Perdida reputacional Perdida de información	Mitigar, mediante la implementación de controles, buscando que la probabilidad de ocurrencia disminuya. Transferir, mediante la contratación de una compañía de seguros	Planillas para registro de eventos que afecten las instalaciones la institución	Políticas sobre uso adecuado de los recursos y la planta física de la institución. ISO 27001: 2013 Dominio 11 Seguridad física y ambiental
INTANGIBLES	Incumplimiento de leyes o regulaciones (propiedad intelectual entre otros). Uso no autorizado de recursos (equipos de comunicación, medios de almacenamiento, sistemas de información, computadores).	Interrupciones en los procesos Retrasos en la ejecución de los procesos	Incumplimiento de normatividades expedidas por el Ministerio de educación Inconformidad del personal	Para en la operación Pérdida de clientes Perdida reputacional	Mitigar, mediante la implementación de controles, buscando que la probabilidad de ocurrencia disminuya.		ISO 27001: 2013 Dominio 17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.

ACTIVO	AMENAZAS	RIESGOS ASOCIADOS	CAUSAS	CONSECUENCIAS	RECOMENDACIONES		CONTROLES ASOCIADOS
					ACCIONES A SEGUIR	MONITOREO	
	Hurto o robo (información, documentos, medios o equipos).	Sanciones administrativas por parte de los estamentos de control.		Perdida de información			ISO 27001: 2013 Dominio 18 Cumplimiento
	Incumplimiento de políticas o procedimientos internos.			Perdidas económicas			

ANEXO I. DECLARACIÓN DE APLICABILIDAD (SoA)

Convenciones (selección de los controles):
L: Requerimiento Regulatorio
N: Requerimiento del negocio
R: Análisis de riesgos

	COLEGIO PRO-COLOMBIANO	**DECLARACIÓN DE APLICABILIDAD (SoA)**	**Versión: 001**					
			Elaboró: Ing. Jerzon Álvarez					
			Vo.Bo: Lic. Rosa Edelmira Salazar					
Objetivo:	**Determinar las decisiones que las directivas tomarán con relación al tratamiento de los riesgos para evitar su materialización o en caso de su materialización, mitigar los impactos que puedan tener en los activos de información de la institución, teniendo como insumo el diagnóstico realizado a la seguridad de la información y al análisis de riesgos identificados a los que se expone la institución, todo esto de conformidad con la norma ISO 27001:2013**							
Anexo A de referencia ISO27001:2013	**Título de control**	**Justificación**	**Aplicar controles**		**Razones para la selección**			
			SI	**NO**	**L**	**N**	**R**	
A.5	**POLITICAS DE SEGURIDAD DE LA INFORMACIÓN**							
A5.1	**Orientación de la dirección para la gestión de la seguridad de la información**	**Para proporcionar a la dirección gestión y apoyo a la seguridad de la información de acuerdo con los requerimientos del negocio y las leyes y reglamentos pertinentes.**						
A.5.1.1	Políticas para la seguridad de la información	El Colegio PRO-COLOMBIANO demuestra su interés hacia la seguridad de la información a través del establecimiento de la política del SGSI y la implementación del SGSI.	**x**		**x**	**x**		

	COLEGIO PRO-COLOMBIANO	**DECLARACIÓN DE APLICABILIDAD (SoA)**	**Versión: 001**					
			Elaboró: Ing. Jerzon Álvarez					
			Vo.Bo: Lic. Rosa Edelmira Salazar					
Objetivo:	**Determinar las decisiones que las directivas tomarán con relación al tratamiento de los riesgos para evitar su materialización o en caso de su materialización, mitigar los impactos que puedan tener en los activos de información de la institución, teniendo como insumo el diagnóstico realizado a la seguridad de la información y al análisis de riesgos identificados a los que se expone la institución, todo esto de conformidad con la norma ISO 27001:2013**							
Anexo A de referencia ISO27001:2013	**Título de control**	**Justificación**	**Aplicar controles**		**Razones para la selección**			
			SI	**NO**	**L**	**N**	**R**	
A.5.1.2	Revisión de las políticas para la seguridad de la información	Asegurar que las políticas se mantienen actualizadas y relacionadas con los requisitos de las partes interesadas y la evaluación del riesgo.	**x**		**x**	**x**	**x**	
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**							
A.6.1	**Organización Interna**							
A.6.1.1	Roles y responsabilidades para la seguridad de la información	Determinar responsabilidades y responsables de la seguridad de los activos d información en los diferentes niveles dentro de la estructura Organizacional de Colegio PRO-COLOMBIANO	**x**			**X**		
A.6.1.2	Separación de deberes	Separar los deberes y áreas de responsabilidad en conflicto para minimizar la modificación y el uso indebido de activos de información.	**x**			**X**		
A.6.1.3	Contacto con las autoridades	Mantener el cumplimiento de la Institución en el contacto con las autoridades pertinentes.	**x**		**x**	**X**		

	COLEGIO PRO-COLOMBIANO	**DECLARACIÓN DE APLICABILIDAD (SoA)**		**Versión: 001**				
				Elaboró: Ing. Jerzon Álvarez				
				Vo.Bo: Lic. Rosa Edelmira Salazar				
Objetivo:	**Determinar las decisiones que las directivas tomarán con relación al tratamiento de los riesgos para evitar su materialización o en caso de su materialización, mitigar los impactos que puedan tener en los activos de información de la institución, teniendo como insumo el diagnóstico realizado a la seguridad de la información y al análisis de riesgos identificados a los que se expone la institución, todo esto de conformidad con la norma ISO 27001:2013**							
Anexo A de referencia ISO27001:2013	**Título de control**	**Justificación**		**Aplicar controles**		**Razones para la selección**		
				SI	**NO**	**L**	**N**	**R**
A.6.1.4	Contacto con grupos de interés especial	Monitorear y estar actualizado respecto a amenazas para la información y sus medios de procesamiento a través de grupos de interés especial.			**x**			
A.6.1.5	Seguridad de la información en la Gestión de Proyectos	Tratar la seguridad de la información en la gestión de proyectos, no importa el tipo de proyecto.		**x**			**X**	
A6.2	**Dispositivos móviles y Teletrabajo.**							
A.6.2.1	Política para dispositivos móviles	Políticas para gestionar los riesgos introducidos por el uso de dispositivos móviles.		**x**			**x**	
A.6.2.2	Teletrabajo	Colegio PRO-COLOMBIANO no tiene establecida la modalidad de Teletrabajo.			**x**			
A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**							
A.7.1	**Antes de Asumir el Empleo**							

	COLEGIO PRO-COLOMBIANO	**DECLARACIÓN DE APLICABILIDAD (SoA)**	**Versión: 001**
			Elaboró: Ing. Jerzon Álvarez
			Vo.Bo: Lic. Rosa Edelmira Salazar
Objetivo:	**Determinar las decisiones que las directivas tomarán con relación al tratamiento de los riesgos para evitar su materialización o en caso de su materialización, mitigar los impactos que puedan tener en los activos de información de la institución, teniendo como insumo el diagnóstico realizado a la seguridad de la información y al análisis de riesgos identificados a los que se expone la institución, todo esto de conformidad con la norma ISO 27001:2013**		

Anexo A de referencia ISO27001:2013	**Título de control**	**Justificación**	**Aplicar controles**		**Razones para la selección**		
			SI	**NO**	**L**	**N**	**R**
A.7.1.1	Selección	Colegio PRO-COLOMBIANO debe contar con procedimientos para la selección de personal que incluye investigación de antecedentes.	**x**			**X**	
A.7.1.2	Términos y condiciones del empleo	Establecer dentro de las obligaciones contractuales de empleados o terceros, condiciones respecto a la seguridad de información.	**x**			**X**	
A.7.2	**Durante la Ejecución del Empleo**						
A.7.2.1	Responsabilidades de la dirección	Es importante que los involucrados en el SGSI tengan claras sus responsabilidades respecto a la seguridad de los activos de información.	**x**			**X**	
A.7.2.2	Toma de conciencia , educación y formación en la seguridad de la información	Colegio PRO-COLOMBIANO debe realizar campañas y actividades que sensibilicen a sus colaboradores sobre la seguridad de la Información.	**x**			**X**	**x**
A.7.2.3	Proceso disciplinario	En caso de no cumplir con los criterios de Seguridad de la información, Colegio PRO-COLOMBIANO debe contar con procesos disciplinarios conforme al marco legal.	**x**			**x**	**x**
A.7.3	**Terminación y cambio de empleo**						

	COLEGIO PRO-COLOMBIANO	DECLARACIÓN DE APLICABILIDAD (SoA)	Versión: 001				
			Elaboró: Ing. Jerzon Álvarez				
			Vo.Bo: Lic. Rosa Edelmira Salazar				
Objetivo:	**Determinar las decisiones que las directivas tomarán con relación al tratamiento de los riesgos para evitar su materialización o en caso de su materialización, mitigar los impactos que puedan tener en los activos de información de la institución, teniendo como insumo el diagnóstico realizado a la seguridad de la información y al análisis de riesgos identificados a los que se expone la institución, todo esto de conformidad con la norma ISO 27001:2013**						
Anexo A de referencia ISO27001:2013	**Título de control**	**Justificación**	**Aplicar controles**		**Razones para la selección**		
			SI	**NO**	**L**	**N**	**R**
A.7.3.1	Terminación o cambio de responsabilidades de empleo	Asegurar la integridad, confidencialidad y disponibilidad de los activos de información durante el proceso de retiro, licencia y movimiento de personal.	**x**			**x**	**x**
A.8	**GESTIÓN DE ACTIVOS**						
A.8.1	**Responsabilidad por los Activos**						
A.8.1.1	Inventario de Activos	Conocer y clasificar los Activos de Información.	**x**			**x**	**x**
A.8.1.2	Propiedad de los activos	Definir responsabilidades sobre la asignación de activos.	**x**			**x**	**x**
A.8.1.3	Uso aceptable de los activos	Contar con políticas para el manejo y uso de recursos tecnológicos	**x**			**x**	**x**
A.8.1.4	Devolución de activos	Asegurar la integridad, confidencialidad y disponibilidad de los activos de información durante el proceso de retiro, renuncia y traslados de personal.	**x**			**x**	**x**
A.8.2	**Clasificación de la Información**						

	COLEGIO PRO-COLOMBIANO	**DECLARACIÓN DE APLICABILIDAD (SoA)**	**Versión: 001**
			Elaboró: Ing. Jerzon Álvarez
			Vo.Bo: Lic. Rosa Edelmira Salazar
Objetivo:	**Determinar las decisiones que las directivas tomarán con relación al tratamiento de los riesgos para evitar su materialización o en caso de su materialización, mitigar los impactos que puedan tener en los activos de información de la institución, teniendo como insumo el diagnóstico realizado a la seguridad de la información y al análisis de riesgos identificados a los que se expone la institución, todo esto de conformidad con la norma ISO 27001:2013**		

Anexo A de referencia ISO27001:2013	**Título de control**	**Justificación**	**Aplicar controles**		**Razones para la selección**		
			SI	**NO**	**L**	**N**	**R**
A.8.2.1	Clasificación de la información	Identificar y clasificar los Activos de Información.	**x**			**x**	**x**
A.8.2.2	Etiquetado de la información	Facilitar el control de la información con el manejo de las etiquetas derivadas de la clasificación de la Información.	**x**			**x**	**x**
A.8.2.3	Manejo de activos	Contar con procedimientos para el manejo de activos de información.	**x**			**x**	**x**
A.8.3	**Manejo de Medios**						
A.8.3.1	Gestión de los medios removibles	En la operación de los procesos dentro del SGSI son utilizados medios electrónicos móviles, por lo que se requiere definir un procedimiento que controle su uso	**x**			**x**	**x**
A.8.3.2	Disposición de los medios	Una vez que los activos de información no vuelvan a ser utilizados o son destinados para fines diferentes a los actuales debe protegerse la información, software y accesos conforme a las políticas correspondientes.	**x**			**x**	**x**
A.8.3.3	Transferencia de medios físicos	Procedimientos para el manejo y almacenamiento de la información que eviten el acceso no autorizado o uso inadecuado de la información de la empresa.	**x**			**x**	**x**

	COLEGIO PRO-COLOMBIANO	**DECLARACIÓN DE APLICABILIDAD (SoA)**	**Versión: 001**					
			Elaboró: Ing. Jerzon Álvarez					
			Vo.Bo: Lic. Rosa Edelmira Salazar					
Objetivo:	**Determinar las decisiones que las directivas tomarán con relación al tratamiento de los riesgos para evitar su materialización o en caso de su materialización, mitigar los impactos que puedan tener en los activos de información de la institución, teniendo como insumo el diagnóstico realizado a la seguridad de la información y al análisis de riesgos identificados a los que se expone la institución, todo esto de conformidad con la norma ISO 27001:2013**							
Anexo A de referencia ISO27001:2013	**Título de control**	**Justificación**	**Aplicar controles**		**Razones para la selección**			
			SI	**NO**	**L**	**N**	**R**	
A.9	**CONTROL DE ACCESO**							
A9.1	**Requisitos del Negocio para el Control de Acceso**							
A9.1.1	Política de control de acceso	Controlar el acceso a la información	**x**			**x**	**x**	
A9.1.2	Acceso a redes y a servicios de red	Asegurar que los usuarios de la red sólo acceden a los servicios para los que están autorizados. * Establecer controles de seguridad que permitan asegurar que los propietarios de activos de información controlan el acceso a la información	**x**			**x**	**x**	
A9.2	**Gestión del Acceso de Usuarios**							
A9.2.1	Registro y cancelación del registro de usuarios	Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información y servicios.	**x**			**x**	**x**	
A9.2.2	Suministro de acceso a usuarios	Asignar o revocar derechos de acceso a usuarios para todos los servicios.	**x**			**x**	**x**	

	COLEGIO PRO-COLOMBIANO	**DECLARACIÓN DE APLICABILIDAD (SoA)**		**Versión: 001**				
				Elaboró: Ing. Jerzon Álvarez				
				Vo.Bo: Lic. Rosa Edelmira Salazar				
Objetivo:	**Determinar las decisiones que las directivas tomarán con relación al tratamiento de los riesgos para evitar su materialización o en caso de su materialización, mitigar los impactos que puedan tener en los activos de información de la institución, teniendo como insumo el diagnóstico realizado a la seguridad de la información y al análisis de riesgos identificados a los que se expone la institución, todo esto de conformidad con la norma ISO 27001:2013**							
Anexo A de referencia ISO27001:2013	**Título de control**	**Justificación**		**Aplicar controles**		**Razones para la selección**		
				SI	**NO**	**L**	**N**	**R**
A9.2.3	Gestión de derechos de acceso privilegiado	El personal de la institución maneja diferentes tipos de información de acuerdo al área o proyecto en el cual participan, por esta razón es muy importante gestionar de forma adecuada el acceso de los usuarios de acuerdo al área o proyecto. Controlar el acceso a la información de los sistemas y servicios.		**x**			**x**	**x**
A9.2.4	Gestión de información de autenticación secreta de usuarios	Controlar el acceso a la información de los sistemas y servicios.		**x**			**x**	**x**
A9.2.5	Revisión de los derechos de acceso de usuarios	Asegurar que cada usuario solamente tenga acceso a la información que requiere para sus funciones.		**x**			**x**	**x**
A9.2.6	Retiro o ajuste de los derechos de acceso	Asegurar la integridad, confidencialidad y disponibilidad de los activos de información durante el proceso de retiro, renuncia y traslado de personal.		**x**			**x**	**x**
A9.3	**Responsabilidades de los Usuarios**							
A9.3.1	Uso de información de autenticación secreta	Usuario único e intransferible al cual se le asignan las respectivas credenciales, las cuales se deben actualizar cada treinta (30 (días) para que realice el envío de reportes al Ministerio de educación.		**x**			**x**	**x**

	COLEGIO PRO-COLOMBIANO	**DECLARACIÓN DE APLICABILIDAD (SoA)**	**Versión: 001**					
			Elaboró: Ing. Jerzon Álvarez					
			Vo.Bo: Lic. Rosa Edelmira Salazar					
Objetivo:	**Determinar las decisiones que las directivas tomarán con relación al tratamiento de los riesgos para evitar su materialización o en caso de su materialización, mitigar los impactos que puedan tener en los activos de información de la institución, teniendo como insumo el diagnóstico realizado a la seguridad de la información y al análisis de riesgos identificados a los que se expone la institución, todo esto de conformidad con la norma ISO 27001:2013**							
Anexo A de referencia ISO27001:2013	**Título de control**	**Justificación**	**Aplicar controles**		**Razones para la selección**			
			SI	**NO**	**L**	**N**	**R**	
A9.4	**Control de Acceso a Sistemas y Aplicaciones**							
A9.4.1	Restricción del acceso a la información	Evitar que usuarios no autorizados tengan acceso a los sistemas de información.	**x**			**x**	**x**	
A9.4.2	Procedimiento de ingreso seguro	Se consideran suficientes los controles y procedimientos implementados para autenticación.	**x**			**x**	**x**	
A9.4.3	Sistema de gestión de contraseñas	Mantener patrón de claves de acceso. Recuperación de contraseñas.	**x**			**x**	**x**	
A9.4.4	Uso de programas utilitarios privilegiados	Se controla el uso de programas utilitarios.	**x**			**x**	**x**	
A9.4.5	Control de acceso al código fuente de los programas	El acceso no permitido a los códigos fuente de los sistemas de la organización puede provocar su robo o que el sistema sea corrompido y verse afectados en su funcionamiento, con el seguro impacto a los clientes.	**x**			**x**	**x**	
A10	**CRIPTOGRAFÍA**							
A10.1	**Controles Criptográficos**							

	COLEGIO PRO-COLOMBIANO	**DECLARACIÓN DE APLICABILIDAD (SoA)**	**Versión: 001**				
			Elaboró: Ing. Jerzon Álvarez				
			Vo.Bo: Lic. Rosa Edelmira Salazar				
Objetivo:	**Determinar las decisiones que las directivas tomarán con relación al tratamiento de los riesgos para evitar su materialización o en caso de su materialización, mitigar los impactos que puedan tener en los activos de información de la institución, teniendo como insumo el diagnóstico realizado a la seguridad de la información y al análisis de riesgos identificados a los que se expone la institución, todo esto de conformidad con la norma ISO 27001:2013**						
Anexo A de referencia ISO27001:2013	**Título de control**	**Justificación**	**Aplicar controles**		**Razones para la selección**		
			SI	**NO**	**L**	**N**	**R**
A10.1.1	Política sobre el uso de controles criptográficos	Desarrollar e implementar controles criptográficos para la protección de la información.	**x**			**x**	**x**
A10.1.2	Gestión de llaves	Implementar sistema de gestión de llaves para apoyar el uso de las técnicas criptográficas.	**x**			**x**	**x**
A11	**SEGURIDAD FÍSICA Y DEL ENTRONO**						
A11.1	**Áreas Seguras**	**Para controlar el acceso a la información.**					
A11.1.1	Perímetro de seguridad física	Limitar la posibilidad de pérdida de activos de información definiendo perímetros de seguridad física.	**x**			**x**	**x**
A11.1.2	Controles de acceso físicos	Evitar el acceso no autorizado a áreas seguras como área de servidores, área de comunicaciones, archivo con información confidencial	**x**			**x**	**x**
A11.1.3	Seguridad de oficinas, recintos e instalaciones	Preservar las áreas de resguardo de activos de información.	**x**			**x**	**x**
A11.1.4	Protección contra amenazas externas y ambientales	Preservar los de activos de información, contra desastres naturales, ataques maliciosos o accidentes. Se cuenta con sistema de aire acondicionado en data center, protección con	**x**			**x**	**x**

	COLEGIO PRO-COLOMBIANO	**DECLARACIÓN DE APLICABILIDAD (SoA)**	**Versión: 001**				
			Elaboró: Ing. Jerzon Álvarez				
			Vo.Bo: Lic. Rosa Edelmira Salazar				
Objetivo:	**Determinar las decisiones que las directivas tomarán con relación al tratamiento de los riesgos para evitar su materialización o en caso de su materialización, mitigar los impactos que puedan tener en los activos de información de la institución, teniendo como insumo el diagnóstico realizado a la seguridad de la información y al análisis de riesgos identificados a los que se expone la institución, todo esto de conformidad con la norma ISO 27001:2013**						
Anexo A de referencia ISO27001:2013	**Título de control**	**Justificación**	**Aplicar controles**		**Razones para la selección**		
			SI	**NO**	**L**	**N**	**R**
		UPS y Planta Eléctrica, protegido con extintores especiales para data center.					
A11.1.5	Trabajo en áreas seguras	Preservar las áreas de resguardo de activos de información y los propios activos de daños no intencionados.	**x**			**x**	**x**
A11.1.6	Áreas de carga, despacho y acceso público	La infraestructura utilizada para el desarrollo de las actividades no cuenta con áreas de carga o despacho, pues no se requiere por las actividades desarrolladas por tal razón no es necesario establecer controles de seguridad para proteger las áreas de despacho o carga.		**x**			
A11.2	**Equipos**						
A11.2.1	Ubicación y protección de los equipos	Prevenir la perdida de activos de información por daño o robo.	**x**				
A11.2.2	Servicios de suministro	Mantener la operación de equipos críticos. Se recomienda contar con plantas o elementos que garanticen la continuidad del suministro eléctrico comercial.		**x**			
A11.2.3	Seguridad del cableado	El cableado de energía eléctrica y de comunicaciones se debe proteger.	**x**			**x**	**x**

	COLEGIO PRO-COLOMBIANO	**DECLARACIÓN DE APLICABILIDAD (SoA)**	**Versión: 001** **Elaboró: Ing. Jerzon Álvarez** **Vo.Bo: Lic. Rosa Edelmira Salazar**
Objetivo:	**Determinar las decisiones que las directivas tomarán con relación al tratamiento de los riesgos para evitar su materialización o en caso de su materialización, mitigar los impactos que puedan tener en los activos de información de la institución, teniendo como insumo el diagnóstico realizado a la seguridad de la información y al análisis de riesgos identificados a los que se expone la institución, todo esto de conformidad con la norma ISO 27001:2013**		

Anexo A de referencia ISO27001:2013	**Título de control**	**Justificación**	**Aplicar controles**		**Razones para la selección**		
			SI	**NO**	**L**	**N**	**R**
A11.2.4	Mantenimiento de los equipos	Mantener la operatividad de los equipos, continuidad de actividades de producción.	**x**			**x**	**x**
A11.2.5	Retiro de activos	Autorización para el retiro de activos.	**x**			**x**	**x**
A11.2.6	Seguridad de los equipos fuera de las instalaciones	Evitar daños o pérdidas a los equipos cuando se encuentran fuera de las instalaciones. (portátiles, discos duros)	**x**			**x**	**x**
A11.2.7	Disposición segura o reutilización de equipos	Evitar fugas de la información propiedad del Colegio PRO-COLOMBIANO, evitar la ocurrencia de eventos como pérdida, daño, robo o interrupción de los equipos tanto dentro como fuera de la organización.	**x**			**x**	**x**
A11.2.8	Equipo de usuario desatendido	Evitar el acceso no autorizado a equipos de cómputo, cuando el usuario no se encuentra.	**x**			**x**	**x**
A11.2.9	Política de escritorio despejado y de pantalla despejada	Evitar acceso o filtraciones de información a través de documentos en áreas visibles.	**x**			**x**	**x**
A12	**SEGURIDAD DE LAS OPERACIONES**						

	COLEGIO PRO-COLOMBIANO	**DECLARACIÓN DE APLICABILIDAD (SoA)**		**Versión: 001**				
				Elaboró: Ing. Jerzon Álvarez				
				Vo.Bo: Lic. Rosa Edelmira Salazar				
Objetivo:	**Determinar las decisiones que las directivas tomarán con relación al tratamiento de los riesgos para evitar su materialización o en caso de su materialización, mitigar los impactos que puedan tener en los activos de información de la institución, teniendo como insumo el diagnóstico realizado a la seguridad de la información y al análisis de riesgos identificados a los que se expone la institución, todo esto de conformidad con la norma ISO 27001:2013**							
Anexo A de referencia ISO27001:2013	**Título de control**	**Justificación**	**Aplicar controles**		**Razones para la selección**			
			SI	**NO**	**L**	**N**	**R**	
A12.1	**Procedimientos Operacionales y Responsabilidades**							
A12.1.1	Procedimientos de operación documentados	Establecer las condiciones de operación conforme a las necesidades de los procesos del Colegio PRO-COLOMBIANO, según aplique.	**x**			**x**	**x**	
A12.1.2	Gestión de cambios	Controlar los cambios que afecten la Seguridad de la Información.	**x**			**x**	**x**	
A12.1.3	Gestión de la capacidad	Gestionar los recursos tecnológicos requeridos para llevar a cabo la operación del Colegio PRO-COLOMBIANO.	**x**			**x**		
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Preservar activos e información de operación / producción ante desarrollos o cambios. La organización realiza antes de la instalación de software pruebas en ambientes diferentes a los de producción con el fin de reducir los riesgos de acceso y cambios no autorizados.	**x**			**x**		
A12.2	**Protección contra Códigos Maliciosos**							

	COLEGIO PRO-COLOMBIANO	**DECLARACIÓN DE APLICABILIDAD (SoA)**		**Versión: 001**				
				Elaboró: Ing. Jerzon Álvarez				
				Vo.Bo: Lic. Rosa Edelmira Salazar				
Objetivo:	**Determinar las decisiones que las directivas tomarán con relación al tratamiento de los riesgos para evitar su materialización o en caso de su materialización, mitigar los impactos que puedan tener en los activos de información de la institución, teniendo como insumo el diagnóstico realizado a la seguridad de la información y al análisis de riesgos identificados a los que se expone la institución, todo esto de conformidad con la norma ISO 27001:2013**							
Anexo A de referencia ISO27001:2013	**Título de control**	**Justificación**		**Aplicar controles**		**Razones para la selección**		
				SI	**NO**	**L**	**N**	**R**
A12.2.1	Controles contra códigos maliciosos	Evitar daños al software y hardware de la Organización con controles contra códigos maliciosos. así como también procedimientos de concientización de los usuarios		**x**				
A12.3	**Copias de Respaldo**							
A12.3.1	Respaldo de la información	Mantener la disponibilidad e integridad de la información. Establecer controles de seguridad que aseguren la ejecución de procedimientos de backup y recuperación que permitan restaurar en el menor tiempo la información ante la materialización de un riesgo, y así permitir que la empresa continué con sus actividades habituales sin ningún inconveniente.		**x**				
A12.4	**Registro y Seguimiento**							
A12.4.1	Registro de eventos	Mantener registro de las operaciones de los usuarios realizadas en las bases de datos. Es importante establecer controles de seguridad que permitan la oportuna detección de actividades de procesamiento de información no autorizadas		**x**			**x**	**x**

	COLEGIO PRO-COLOMBIANO	**DECLARACIÓN DE APLICABILIDAD (SoA)**			**Versión: 001**			
					Elaboró: Ing. Jerzon Álvarez			
					Vo.Bo: Lic. Rosa Edelmira Salazar			
Objetivo:	**Determinar las decisiones que las directivas tomarán con relación al tratamiento de los riesgos para evitar su materialización o en caso de su materialización, mitigar los impactos que puedan tener en los activos de información de la institución, teniendo como insumo el diagnóstico realizado a la seguridad de la información y al análisis de riesgos identificados a los que se expone la institución, todo esto de conformidad con la norma ISO 27001:2013**							
Anexo A de referencia ISO27001:2013	**Título de control**	**Justificación**	**Aplicar controles**		**Razones para la selección**			
			SI	**NO**	**L**	**N**	**R**	
		y herramientas para investigaciones futuras de incidentes de seguridad de la información.						
A12.4.2	Protección de la información de registro	Mantener y proteger el historial de logs.	**x**			**x**	**x**	
A12.4.3	Registros del administrador y del operador	Mantener registro de las operaciones realizadas.		**x**				
A12.4.4	Sincronización de relojes	Asegurar la hora exacta de las transacciones de los servidores.		**x**				
A12.5	**Control de Software Operacional**							
A12.5.1	Instalación de software en sistemas operativos	Para mantener la seguridad de software de sistema de aplicación y la información**.** Controlar accesos para instalación de software en los sistemas operativos.	**x**			**x**		
A12.6	**Gestión de Vulnerabilidades Técnica**							
A12.6.1	Gestión de las vulnerabilidades técnicas	Para reducir los riesgos derivados de la explotación de las vulnerabilidades técnicas. Los nuevos sistemas de información deben especificar los requerimientos de controles de seguridad necesarios para cumplir los lineamientos en materia de seguridad del negocio. Es necesario establecer	**x**			**x**		

	COLEGIO PRO-COLOMBIANO	**DECLARACIÓN DE APLICABILIDAD (SoA)**		**Versión: 001**				
				Elaboró: Ing. Jerzon Álvarez				
				Vo.Bo: Lic. Rosa Edelmira Salazar				
Objetivo:	**Determinar las decisiones que las directivas tomarán con relación al tratamiento de los riesgos para evitar su materialización o en caso de su materialización, mitigar los impactos que puedan tener en los activos de información de la institución, teniendo como insumo el diagnóstico realizado a la seguridad de la información y al análisis de riesgos identificados a los que se expone la institución, todo esto de conformidad con la norma ISO 27001:2013**							
Anexo A de referencia ISO27001:2013	**Título de control**	**Justificación**		**Aplicar controles**		**Razones para la selección**		
				SI	**NO**	**L**	**N**	**R**
		controles de seguridad para garantizar la reducción de los riesgos derivados de las vulnerabilidades técnicas.						
A12.6.2	Restricción sobre la instalación de software	La organización para el desarrollo de sus actividades utiliza diferentes sistemas operativos, en tal sentido es importante establecer controles de seguridad para garantizar la protección, control y correcta operación de los sistemas operativos.					**x**	
A12.7	**Consideraciones sobre Auditorias de Sistemas de Información**							
A12.7.1	Controles de auditorías de sistemas de información	Realizar auditorías para verificar los sistemas operativos para minimizar las interrupciones en los procesos. Establecer controles de seguridad que garanticen un adecuado uso de las herramientas de auditoria y minimizar la interrupción de los sistemas durante el proceso.			**x**			
A13	**SEGURIDAD DE LAS COMUNICACIONES**							
A13.1	**Gestión de la Seguridad de las Redes**							

	COLEGIO PRO-COLOMBIANO	**DECLARACIÓN DE APLICABILIDAD (SoA)**	**Versión: 001**
			Elaboró: Ing. Jerzon Álvarez
			Vo.Bo: Lic. Rosa Edelmira Salazar
Objetivo:	**Determinar las decisiones que las directivas tomarán con relación al tratamiento de los riesgos para evitar su materialización o en caso de su materialización, mitigar los impactos que puedan tener en los activos de información de la institución, teniendo como insumo el diagnóstico realizado a la seguridad de la información y al análisis de riesgos identificados a los que se expone la institución, todo esto de conformidad con la norma ISO 27001:2013**		

Anexo A de referencia ISO27001:2013	**Título de control**	**Justificación**	**Aplicar controles**		**Razones para la selección**		
			SI	**NO**	**L**	**N**	**R**
A13.1.1	Controles de las redes	Gestión y control de las redes para proteger información en sistemas y aplicaciones	**x**			**x**	**x**
A13.1.2	Seguridad de los servicios de red	Asegurar los servicios en red.	**x**			**x**	**x**
A13.1.3	Separación en las redes	Evitar que el tráfico de una red o subred afecte a las demás.	**x**			**x**	**x**
A13.2	**Transferencia de Información**						
A13.2.1	Políticas y procedimientos para el intercambio de información	Establecer los mecanismos de intercambio de información entre dependencias del Colegio PRO-COLOMBIANO, que asegure la confidencialidad, integridad y disponibilidad de los datos.	**x**			**x**	**x**
A13.2.2	Acuerdos sobre transferencia de información	Asegurar la confidencialidad de la información, en manos de terceras partes para garantizar que no se presente uso inadecuado o corrupción cuando la información sale fuera de las instalaciones de la organización.	**x**			**x**	**x**

	COLEGIO PRO-COLOMBIANO	**DECLARACIÓN DE APLICABILIDAD (SoA)**	**Versión: 001**
			Elaboró: Ing. Jerzon Álvarez
			Vo.Bo: Lic. Rosa Edelmira Salazar
Objetivo:	**Determinar las decisiones que las directivas tomarán con relación al tratamiento de los riesgos para evitar su materialización o en caso de su materialización, mitigar los impactos que puedan tener en los activos de información de la institución, teniendo como insumo el diagnóstico realizado a la seguridad de la información y al análisis de riesgos identificados a los que se expone la institución, todo esto de conformidad con la norma ISO 27001:2013**		

Anexo A de referencia ISO27001:2013	**Título de control**	**Justificación**	**Aplicar controles**		**Razones para la selección**		
			SI	**NO**	**L**	**N**	**R**
A13.2.3	Mensajería electrónica	Evitar accesos no autorizados al servidor de correo IDS, buzones de correo. Evitar la recepción de correo no solicitado (SPAM). Mantener la disponibilidad del servicio. Evitar transmisión de virus.	**x**			**x**	**x**
A13.2.4	Acuerdos de confidencialidad o de no divulgación	Asegurar la confidencialidad y garantizar la protección de la información.	**x**			**x**	**x**
A14	**ADQUISISCIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN**						
A14.1	**Requisitos de Seguridad de los Sistemas de Información**						
A14.1.1	Análisis y especificación de los requisitos de seguridad de la información	Los nuevos sistemas de información deben especificar los requerimientos de controles de seguridad necesarios para cumplir los lineamientos en materia de seguridad del negocio.	**x**			**x**	**x**
A14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Proteger de actividades fraudulentas la información de los servicios que utilizan redes públicas.	**x**			**x**	**x**

	COLEGIO PRO-COLOMBIANO	**DECLARACIÓN DE APLICABILIDAD (SoA)**		**Versión: 001**				
				Elaboró: Ing. Jerzon Álvarez				
				Vo.Bo: Lic. Rosa Edelmira Salazar				
Objetivo:	**Determinar las decisiones que las directivas tomarán con relación al tratamiento de los riesgos para evitar su materialización o en caso de su materialización, mitigar los impactos que puedan tener en los activos de información de la institución, teniendo como insumo el diagnóstico realizado a la seguridad de la información y al análisis de riesgos identificados a los que se expone la institución, todo esto de conformidad con la norma ISO 27001:2013**							
Anexo A de referencia ISO27001:2013	**Título de control**	**Justificación**		**Aplicar controles**		**Razones para la selección**		
				SI	**NO**	**L**	**N**	**R**
A14.1.3	Protección de transacciones de los servicios de las aplicaciones	Evitar la transmisión incompleta, el enrutamiento errado, alteración, divulgación, duplicación o reproducción de mensajes no autorizada (criptografía).		**x**			**x**	**x**
A14.2	**Seguridad en los Procesos de Desarrollo y Soporte**							
A14.2.1	Política de desarrollo seguro	Establecer políticas para desarrollo de productos de software.			**x**			
A14.2.2	Procedimientos de control de cambios en sistemas	Es esencial, para evitar que los cambios se realicen de forma no controlada, que se cuente con un procedimiento que establezca los pasos a seguir para que los cambios a los sistemas se hagan de manera ordenada y correcta.			**x**			
A14.2.3	Revisión técnica de las aplicaciones después de los cambios en la plataforma de operación	Se deben probar los cambios en los sistemas previos a su distribución para asegurar que no tengan un impacto adverso a las operaciones de la organización o a su seguridad o del cliente final.			**x**			
A14.2.4	Restricciones en los cambios a los paquetes de software	Los cambios en los sistemas deben ser restringidos para evitar las modificaciones fuera de control que podrían generar fallas no deseadas o conocidas.			**x**			

	COLEGIO PRO-COLOMBIANO	**DECLARACIÓN DE APLICABILIDAD (SoA)**	**Versión: 001**
			Elaboró: Ing. Jerzon Álvarez
			Vo.Bo: Lic. Rosa Edelmira Salazar
Objetivo:	**Determinar las decisiones que las directivas tomarán con relación al tratamiento de los riesgos para evitar su materialización o en caso de su materialización, mitigar los impactos que puedan tener en los activos de información de la institución, teniendo como insumo el diagnóstico realizado a la seguridad de la información y al análisis de riesgos identificados a los que se expone la institución, todo esto de conformidad con la norma ISO 27001:2013**		

Anexo A de referencia ISO27001:2013	**Título de control**	**Justificación**	**Aplicar controles**		**Razones para la selección**		
			SI	**NO**	**L**	**N**	**R**
A14.2.5	Principios de construcción de los sistemas seguros	Establecer, documentar y mantener políticas para desarrollo de aplicaciones de software seguros y aplicarlos en cualquier actividad de implementación.		**x**			
A14.2.6	Ambiente de desarrollo seguro	Garantizar ambientes de desarrollo seguros para todas las actividades del ciclo de vida de desarrollo de productos de software (***ambientes de desarrollo simulado, entornos similares al de los clientes***).		**x**			
A14.2.7	Desarrollo contratado externamente	Validar el procesamiento de los sistemas antes de ponerlos en producción, en caso de contratar compañías externas.		**x**			
A14.2.8	Pruebas de seguridad de sistemas	Realizar pruebas de seguridad durante el desarrollo.		**x**			
A14.2.9	Prueba de aceptación del sistema	Determinar la posible afectación a la operación del Colegio PRO-COLOMBIANO y de la entrega de producto de calidad a los clientes, adicional al adecuado uso de los recursos.		**x**			
A14.3	**Datos de Prueba**						

	COLEGIO PRO-COLOMBIANO	**DECLARACIÓN DE APLICABILIDAD (SoA)**			**Versión: 001**			
					Elaboró: Ing. Jerzon Álvarez			
					Vo.Bo: Lic. Rosa Edelmira Salazar			
Objetivo:	**Determinar las decisiones que las directivas tomarán con relación al tratamiento de los riesgos para evitar su materialización o en caso de su materialización, mitigar los impactos que puedan tener en los activos de información de la institución, teniendo como insumo el diagnóstico realizado a la seguridad de la información y al análisis de riesgos identificados a los que se expone la institución, todo esto de conformidad con la norma ISO 27001:2013**							
Anexo A de referencia ISO27001:2013	**Título de control**	**Justificación**	**Aplicar controles**		**Razones para la selección**			
			SI	**NO**	**L**	**N**	**R**	
A14.3.1	Protección de los datos de prueba del sistema	Se deben seleccionar cuidadosamente los datos que se van a utilizar en las pruebas para evitar alguna fuga de la información.		**x**				
A15	**RELACIONES CON LOS PROVEEDORES**							
A15.1	**Seguridad de la Información en las Relaciones con los Proveedores**							
A15.1.1	Política de seguridad de la información para las relaciones con proveedores	Se debe establecer controles de seguridad para garantizar que se tiene en cuenta los requisitos del negocio antes de gestionar compras de bienes o servicios que afecten la seguridad de la información de la organización y la infraestructura que sobre la cual esta soportada.	**x**			**x**		
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Establecer y acordar requisitos de seguridad de la información con los proveedores.	**x**			**x**		
A15.1.3	Cadena de suministro de tecnología de información y comunicación	Los acuerdos con terceros deben incluir requisitos para tratar los riesgos de seguridad de la información.	**x**			**x**		
A15.2	**Gestión de la Prestación del Servicios de Proveedores**							

	COLEGIO PRO-COLOMBIANO	**DECLARACIÓN DE APLICABILIDAD (SoA)**	**Versión: 001**					
			Elaboró: Ing. Jerzon Álvarez					
			Vo.Bo: Lic. Rosa Edelmira Salazar					
Objetivo:	**Determinar las decisiones que las directivas tomarán con relación al tratamiento de los riesgos para evitar su materialización o en caso de su materialización, mitigar los impactos que puedan tener en los activos de información de la institución, teniendo como insumo el diagnóstico realizado a la seguridad de la información y al análisis de riesgos identificados a los que se expone la institución, todo esto de conformidad con la norma ISO 27001:2013**							
Anexo A de referencia ISO27001:2013	**Título de control**	**Justificación**	**Aplicar controles**		**Razones para la selección**			
			SI	**NO**	**L**	**N**	**R**	
A15.2.1	Seguimiento y revisión de los servicios de los proveedores	Determinar el grado de cumplimiento de terceras partes conforme contrato y/o acuerdos.	**x**			**x**		
A15.2.2	Gestión de cambios en los servicios de los proveedores	Es necesario establecer controles de seguridad para garantizar que tienen en cuenta los requisitos del negocio antes de gestionar compras de bienes o servicios que afecten la seguridad de la información e la organización y la infraestructura que sobre la cual esta soportada.	**x**			**x**		
A16	**GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN**							
A16.1	**Gestión de los Incidentes y las Mejoras en la Seguridad de la Información**							
A16.1.1	Responsabilidades y procedimientos	Asegurar una respuesta oportuna, efectiva y organizada de los incidentes de seguridad de la información.	**x**			**x**	**x**	

	COLEGIO PRO-COLOMBIANO	**DECLARACIÓN DE APLICABILIDAD (SoA)**	**Versión: 001** **Elaboró: Ing. Jerzon Álvarez** **Vo.Bo: Lic. Rosa Edelmira Salazar**
Objetivo:	**Determinar las decisiones que las directivas tomarán con relación al tratamiento de los riesgos para evitar su materialización o en caso de su materialización, mitigar los impactos que puedan tener en los activos de información de la institución, teniendo como insumo el diagnóstico realizado a la seguridad de la información y al análisis de riesgos identificados a los que se expone la institución, todo esto de conformidad con la norma ISO 27001:2013**		

Anexo A de referencia ISO27001:2013	**Título de control**	**Justificación**	**Aplicar controles**		**Razones para la selección**		
			SI	**NO**	**L**	**N**	**R**
A16.1.2	Reporte sobre los eventos de seguridad de la información	Asegurar que los eventos e incidentes de seguridad de información sean reportados oportunamente.	**x**			**x**	**x**
A16.1.3	Reporte sobre las debilidades en la seguridad	Asegurar que los eventos e incidentes de seguridad de información sean reportados oportunamente.	**x**			**x**	**x**
A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Evaluar los eventos de seguridad de la información y decidir si se clasifican como incidentes de seguridad de la información.	**x**			**x**	**x**
A16.1.5	Respuesta a incidentes de seguridad de la información	Procedimiento para atender incidentes de seguridad de la información.	**x**			**x**	**x**
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Conocimiento adquirido sobre los eventos de seguridad.	**x**			**x**	**x**
A16.1.7	Recolección de evidencias	Mantener las evidencias de los incidentes de seguridad de la información.	**x**			**x**	**x**
A17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**						
A17.1	**Continuidad de Seguridad de la Información**						

	COLEGIO PRO-COLOMBIANO	**DECLARACIÓN DE APLICABILIDAD (SoA)**	**Versión: 001**
			Elaboró: Ing. Jerzon Álvarez
			Vo.Bo: Lic. Rosa Edelmira Salazar
Objetivo:	**Determinar las decisiones que las directivas tomarán con relación al tratamiento de los riesgos para evitar su materialización o en caso de su materialización, mitigar los impactos que puedan tener en los activos de información de la institución, teniendo como insumo el diagnóstico realizado a la seguridad de la información y al análisis de riesgos identificados a los que se expone la institución, todo esto de conformidad con la norma ISO 27001:2013**		

Anexo A de referencia ISO27001:2013	**Título de control**	**Justificación**	**Aplicar controles**		**Razones para la selección**		
			SI	**NO**	**L**	**N**	**R**
A17.1.1	Planificación de la continuidad de la seguridad de la información	Colegio PRO-COLOMBIANO está comprometido con sus clientes a través de los contratos de los proyectos a garantizar el cumplimiento total del objeto de estos, por tal razón se debe implementar un Plan de Continuidad del Negocio que debe estar elaborado con base en los lineamientos y requerimientos de la seguridad y debe estar sujeto a pruebas, escalamiento y pruebas.	**x**		**x**	**x**	**x**
A17.1.2	Implementación de la continuidad de la seguridad de la información	Contar con procedimientos que permitan hacer frente a contingencias y restablecer en el menor tiempo posible los servicios, disminuyendo el impacto que pueda tener para la institución y sus clientes.	**x**		**x**	**x**	**X**
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	El Plan de Continuidad del Negocio debe recibir mantenimiento para que se encuentre actualizado al momento de ser probado y se encuentre apegado a la realidad de las operaciones en la organización.	**x**		**x**	**x**	**x**
A17.2	**Redundancias**						

	COLEGIO PRO-COLOMBIANO	**DECLARACIÓN DE APLICABILIDAD (SoA)**	**Versión: 001**
			Elaboró: Ing. Jerzon Álvarez
			Vo.Bo: Lic. Rosa Edelmira Salazar
Objetivo:	**Determinar las decisiones que las directivas tomarán con relación al tratamiento de los riesgos para evitar su materialización o en caso de su materialización, mitigar los impactos que puedan tener en los activos de información de la institución, teniendo como insumo el diagnóstico realizado a la seguridad de la información y al análisis de riesgos identificados a los que se expone la institución, todo esto de conformidad con la norma ISO 27001:2013**		

Anexo A de referencia ISO27001:2013	**Título de control**	**Justificación**	**Aplicar controles**		**Razones para la selección**		
			SI	**NO**	**L**	**N**	**R**
A17.2.1	Disponibilidad de instalaciones de procesamiento de información	Implementar con redundancia suficientes, las instalaciones de procesamiento de información para Cumplir con el requisito de disponibilidad	**x**			**x**	**x**
A18	**CUMPLIMIENTO**						
A18.1	**Cumplimiento de los Requisitos Legales y Contractuales**						
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	La organización desarrolla sus actividades en el marco del cumplimiento de la legislación Colombiana, los requisitos contractuales y los propios.	**x**		**x**	**x**	**x**
A18.1.2	Derechos de propiedad intelectual (DPI)	Asegurar el cumplimiento de los requisitos legislativos de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	**x**		**x**	**x**	**x**
A18.1.3	Protección de registros	Proteger los registros contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada.	**x**		**x**	**x**	**x**

	COLEGIO PRO-COLOMBIANO	**DECLARACIÓN DE APLICABILIDAD (SoA)**		**Versión: 001**				
				Elaboró: Ing. Jerzon Álvarez				
				Vo.Bo: Lic. Rosa Edelmira Salazar				
Objetivo:	**Determinar las decisiones que las directivas tomarán con relación al tratamiento de los riesgos para evitar su materialización o en caso de su materialización, mitigar los impactos que puedan tener en los activos de información de la institución, teniendo como insumo el diagnóstico realizado a la seguridad de la información y al análisis de riesgos identificados a los que se expone la institución, todo esto de conformidad con la norma ISO 27001:2013**							
Anexo A de referencia ISO27001:2013	**Título de control**	**Justificación**		**Aplicar controles**		**Razones para la selección**		
				SI	**NO**	**L**	**N**	**R**
A18.1.4	Privacidad y protección de información de datos personales	Cuidar las bases de datos y expedientes con datos personales como parte de las buenas prácticas de seguridad para evitar violar los derechos de seguridad en la información y ocasionar daños al personal o a los clientes.		**x**		**x**	**x**	**x**
A18.1.5	Reglamentación de los controles criptográficos	Utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes con el objetivo de garantizar la confidencialidad e integridad de la información.		**x**		**x**	**x**	**x**
A18.2	**Revisiones de Seguridad de la Información**							
A18.2.1	Revisión independiente de la seguridad de la información	El SGSI se debe revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.		**x**		**x**	**x**	**x**
A18.2.2	Cumplimiento con las políticas y las normas de seguridad	Necesaria la inclusión de la Alta Dirección en este proceso, como requisito de la norma y condición de éxito del Sistema de Gestión de Seguridad de la Información. Es importante establecer controles de seguridad que garanticen que todo el personal de la empresa conoce y aplica las políticas de seguridad de la información y los respectivos controles.		**x**		**x**	**x**	**x**

	COLEGIO PRO-COLOMBIANO	**DECLARACIÓN DE APLICABILIDAD (SoA)**	**Versión: 001** **Elaboró: Ing. Jerzon Álvarez** **Vo.Bo: Lic. Rosa Edelmira Salazar**
Objetivo:	**Determinar las decisiones que las directivas tomarán con relación al tratamiento de los riesgos para evitar su materialización o en caso de su materialización, mitigar los impactos que puedan tener en los activos de información de la institución, teniendo como insumo el diagnóstico realizado a la seguridad de la información y al análisis de riesgos identificados a los que se expone la institución, todo esto de conformidad con la norma ISO 27001:2013**		

Anexo A de referencia ISO27001:2013	**Título de control**	**Justificación**	**Aplicar controles**		**Razones para la selección**		
			SI	**NO**	**L**	**N**	**R**
A18.2.3	Revisión del cumplimiento técnico	Controles y aplicaciones técnicas cumplan con requisitos mínimos de seguridad.	**x**		**x**	**x**	**x**

ANEXO J. MANUAL SGSI COLEGIO PRO-COLOMBIANO

MANUAL SGSI PARA EL COLEGIO PRO-COLOMBIANO

CARRERA 19 # 56-83 SUR

Carrera 19 # 56-83 sur

Contenido

1. PRESENTACIÓN

Nombre de la institución:	COLEGIO PRO-COLOMBIANO
Sector:	PRIVADO
Carácter:	MIXTO
Modalidad:	BASICA PRIMARIA
Tipo de educación.	FORMAL
Código del DANE:	311001026491
Inscripción S.E.:	2560
Jornada:	UNICA
Legalización:	Res.5464 DEL 30 DE DICIEMBRE DE 1994

El Colegio Pro-Colombiano, tiene una propuesta educativa basada en principios específicos que busquen la enseñanza y rescate de algunos valores para que se trabaje en la búsqueda de soluciones a situaciones de abuso, violencia e irrespeto, cuyo producto final sea crear un espacio amable un sitio único y agradable donde sea posible construir la felicidad enmarcada por una convivencia social pacífica y el respeto por los derechos humanos.

Además el colegio tiene unos principios rectos que giran en torno a la persona como la única razón de ser de la educación. Por tanto son elementos con validez a largo plazo y aplicables a contextos culturales amplios.

Los estudiantes y los padres de familia constatan y valoran la formación moral y el respeto a la persona enmarcada por la libertad de culto; Además nota que hay empeño en la formación de valores, derechos humanos especialmente en la responsabilidad, tolerancia, verdad, benevolencia, respeto y la solidaridad.

El contexto de funcionamiento hace que se manipule a diario información confidencial, llámese datos personales de alumnos, padres de familia, personal docente, adicional a las calificaciones de los alumnos; esto pone en evidencia que la institución debe ser responsable por el aseguramiento de la información en su resguardo mediante la implementación de políticas y procedimientos que certifiquen su protección aceptando, reduciendo, evitando o transfiriendo los riesgos que puedan comprometer su confidencialidad, integridad y disponibilidad.

2. OBJETIVO

El objetivo del presente Manual es dar a conocer a las directivas de la institución educativa colegio PRO-COLOMBIANO los lineamientos y acciones a seguir para la implementación de un Sistema de Gestión de Seguridad de la Información, en adelante denominado SGSI, con el propósito de minimizar las vulnerabilidades y amenazas de seguridad de la información presentes en la institución.

3. ALCANCE

El alcance del presente manual está encaminado a los procesos de matrícula y procesamiento de las calificaciones de los alumnos de la institución y será de estricto cumplimiento para todos los funcionarios directos y personal externo que le aporte algún bien o servicio a la institución educativa colegio PRO-COLOMBIANO.

4. CONTROL DEL MANUAL

Este documento es propiedad exclusiva de la institución educativa colegio PRO-COLOMBIANO y está prohibida su distribución o copia sin previa autorización de los responsables quienes velaran por su distribución y control y evitar que se realicen modificaciones ni actualizaciones no autorizadas.

5. TERMINOS Y DEFINICIONES

5.1. PRINCIPIOS FUNDAMENTALES DE SEGURIDAD DE LA INFORMACIÓN

Principio disponibilidad: Establece que la información debe estar disponible en todo momento para ser usada o vista solo por personal autorizado.

Principio integridad: Establece que se debe salvaguardar la exactitud y el estado completo de los activos de información, lo que indica que la información solo pueda ser modificada por personal autorizado.

Principio confidencialidad: Establece que la información solo debe estar disponible a individuos, entidades o procesos autorizados garantizando que esta no sea revelada.

5.2. DEFINICIONES

Activo de Información: Conocimientos o datos que tienen valor para la Institución.

Información: Todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

Seguridad de la Información: Es la preservación de la Confidencialidad, Integridad y Disponibilidad de la información Institucional y. Preservación de la confidencialidad, integridad y disponibilidad de la información para propender por la autenticidad, trazabilidad, no repudio y fiabilidad de la misma.

Sistema de Gestión de la Seguridad de la Información (SGSI): Parte del sistema de gestión global, basada en un enfoque hacia los riesgos del negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

Riesgo de Seguridad de la Información: Posibilidad que una amenaza dada explote vulnerabilidades de un activo o de un grupo de activos y por lo tanto cause daño a la Institución.

Integridad: Propiedad de salvaguardar la exactitud y completitud de los activos.

Sistema de Gestión: Marco de políticas, procedimientos, guías y recursos asociados para lograr los objetivos de la Institución.

Políticas: Intenciones globales y orientación tal como se expresan formalmente por la dirección.

Acción Preventiva: Acción tomada para eliminar la causa de una no conformidad potencial u otra situación potencial no deseable.

Procedimiento: Forma especificada para llevar a cabo una actividad o un proceso.

Registro: Documento que presenta resultados obtenidos o proporciona evidencias de actividades desempeñadas.

Riesgo: Combinación de la probabilidad de un evento y de su consecuencia.

Aceptación del Riesgo: Decisión de aceptar un riesgo**.**

Análisis del Riesgo: Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Gestión del Riesgo: Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

6. COMPROMISO DE LA DIRECCIÓN

La directiva del colegio PRO-COLOMBIANO está comprometida con la Seguridad de la Información al acoger integralmente los principios de esta, formulados en la Norma ISO 27002 guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.

Se compromete a resguardar sus activos de información, protegiéndolos de las amenazas que atenten contra ellos, mediante la adecuada gestión del riesgo, el cumplimiento de requisitos legales, mejores prácticas e implementación de controles.

7. PLANIFICACIÓN DEL SGSI

Para el desarrollo y la implementación del Sistema de Gestión de Seguridad de la Información se determinan las siguientes etapas:

- Documentar el sistema
- Implementar el sistema
- Evaluar el sistema a través de auditorías internas y externas
- Mejorar continuamente la eficacia del sistema a través de del análisis de datos.

8. REQUISISTOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Se requiere ajustar el SGSI acorde a las exigencias que determina la normatividad, en este caso el estándar ISO 27001.

8.1. GENERALES

En el presente documento se especifica la forma como se debe establecer, implementar, operar, mantener y mejorar constantemente la eficacia del SGSI, acorde a los requerimientos definidos en los estándares ISO/IEC 27001:2013e **ISO 27003** guía para la implantación de un SGSI..

Cabe anotar que aplican a todo tipo de Organizaciones, independientemente de su tipo, tamaño o área de actividad.

Estos requerimientos son:

- Definición del alcance del SGSI
- Definición de una Política de Seguridad
- Definición de una metodología y criterios para el Análisis y Gestión del Riesgo
- Identificación de riesgos
- Evaluación de los posibles tratamientos del riesgo
- Elaboración de una Declaración de Aplicabilidad de controles y requisitos
- Desarrollo de un Plan de Tratamiento de Riesgos
- Definición de métricas e indicadores de la eficiencia de los controles
- Desarrollo de programas de formación y concienciación en seguridad de la información
- Gestión de recursos y operaciones
- Gestión de incidencias
- Elaboración de procedimientos y documentación asociada

8.2. ESTABLECIMIENTO DEL SGSI

Mediante el establecimiento del SGSI se busca determinar qué mecanismos se utilizarán para preservar la confidencialidad, integridad y disponibilidad de la información, garantizando la protección de los datos de los estudiantes, padres de familia, y empleados de la institución educativa colegio PRO-COLOMBIANO así como la información generada en los procesos de calificaciones, garantizando la eficiencia y transparencia de los procesos llevados a cabo en la institución.

Lo cual se logrará mediante los siguientes procedimientos:

- Iidentificar, administrar y tratar los riesgos de seguridad de las informaciones relevantes a la Institución, de acuerdo a lo especificado en la metodología de identificación, análisis y evaluación de riesgos, para la institución se determinó la utilización de Magerit.
- Gestionarlos incidentes relacionados con la seguridad de la información.
- Divulgar y tener siempre disponibles las políticas y procedimientos de seguridad diseñadas para garantizar que sean comprendidas y utilizadas por los empleados de la institución,
- Capacitar a los empleados en temas de seguridad de la información para fortalecer sus valores éticos y garantizar su compromiso de velar por protección de los activos de información.
- Asegurar la disponibilidad de los activos de información a quien lo requiera y esté debidamente autorizado.
- Garantizar el aprovisionamiento de los recursos necesariospara establecer, implementar, operar monitorear, revisar, mantener y mejorar el SGSI.

8.3. DOCUMENTACIÓN

El colegio PRO-COLOMBIANO debe contar con la siguiente documentación, la cual garantizará la confidencialidad, integridad y disponibilidad de la información asociada al SGSI.

- Autorización y compromiso de la dirección con el SGSI
- Manual del SGSI el cual define su alcance del SGSI.
- Política del SGSI
- Metodología de evaluación del riesgo.
- Informe de la evaluación del riesgo.
- Plan de Tratamiento del riesgo.
- Declaración de aplicabilidad (SoA).
- Registros que proporcionan evidencia del correcto funcionamiento del SGSI.

9. RESPONSABILIDAD DE LA DIRECCIÓN

Es fundamental definir roles y responsables para apoyar y cumplir la política de seguridad de la información, a continuación se relacionan y describen.

9.1. COMPROMISO DE LA DIRECCIÓN

Las directivas d la institución educativa colegio PRO-COLOMBIANO manifiestan su

compromiso con el sistema de gestión de seguridad de la información mediante las siguientes acciones

- Definiendo y estableciendo la política y los objetivos de seguridad de la información y dándolos a conocer a todos los empleados de la institución
- Estableciendo el SGSI al interior de la institución, evaluando su efectividad para propender por su mejora continua.
- Asignando responsabilidades, especificando funciones, delegando y asignando al responsable de la dirección.
- Determinando los criterios de aceptación de los riesgos de seguridad de la información así como los niveles de riesgo aceptables
- Estimulando en los empleados al cumplimiento de las normatividades, requisitos y reglamentos aplicables para garantizar la seguridad de la información.

9.2. RESPONSABILIDADES

9.2.1. Comité SGSI: se encarga de

- Planear, crear, mantener, revisar, auditar y mejorar el sistema, acorde a lo establecido en el estándar ISO/27001:2013.
- Dirigir y verificar los avances y la eficacia del SGSI, teniendo como indicadores los objetivos y metas propuestas y resultado de auditorías internas.
- Vigilar que se cumplan las políticas, normas y procedimientos de seguridad de la información.
- Evaluar y validar las normas, procedimientos, métodos y controles definidos para la seguridad de la información.
- Evaluar la efectividad de los controles y salvaguardas.
- Plantear planes y capacitaciones con el propósito de concientizar al personal acerca de la seguridad de la información
- Planear y definir las acciones a seguir que garanticen la continuidad

de los procesos críticos en caso de presentarse situaciones imprevistas que afecten la seguridad de la información y el normal funcionamiento de las actividades de la institución.

En la institución estará conformado por:

- Representante legal
- Usuario de servicios de información
- Administrador de seguridad informática
- Especialista de seguridad de la información (opcional)

9.2.2. Propietario de activo de información: se encarga de

- Clasificar la información de acuerdo a los niveles de clasificación definidos en la institución.
- Establecer para los usuarios que niveles de acceso tendrán autorizados sobre la información.
- Autorizar la asignación de niveles de acceso sobre la información.
- Definir y asegurar la implementación de controles tendientes a la protección de los activos
- Revisar periódicamente los accesos y privilegios otorgados sobre la información.
- Velar por que se garantice la integridad, confidencialidad y disponibilidad de la información.

9.2.3. Usuarios de la información: Son responsables de:

- Emplear solo para fines autorizados la información sobre la cual tienen acceso autorizado.
- Cumplir con las medidas de seguridad que en la institución se tengan establecidas y definidas en las políticas, normas y procedimientos de seguridad de la información.

- Reportar de manera oportuna cualquier violación de las políticas y normas de seguridad de la que tengan conocimiento.
- Usar los sistemas de información y la red solo para propósitos autorizados e inherentes a la función asignada.

10. GESTIÓN DE RECURSOS

Las directivas de la institución serán responsables de garantizar los recursos necesarios para la implementación, mantenimiento y mejoramiento continuo del SGSI, para lo cual deben garantizar:

- Partida presupuestal: asignando los recursos necesarios que garanticen que se implemente, mantenga y mejore el SGSI.
- Recurso humano especializado: programando capacitaciones y campañas de concientización a los empleados de la institución en el sentido del buen uso, resguardo y protección de la información.

11. POLITICAS

Son de obligatorio cumplimiento para todos los funcionarios de la institución y tienen el propósito de establecer las acciones encaminadas a la protección de la información al interior del colegio PRO-COLOMBIANO.

Estas políticas se presentan como anexos a este manual.

12. MEDICIÓN Y MEJORA

La institución educativa colegio PRO-COLOMBIANO diseña y establece los procesos de revisión y mejora necesarios del SGSI con el propósito de:

- Asegurar la eficacia del Sistema de Gestión de Seguridad de la Información
- Optimizarla eficiencia del SGSI.

Lo cual se logra mediante:

A. Revisión por parte de la dirección

Anualmente las directivas de la institución realizarán la revisión del SGSI con el propósito de:

- Asegurar su eficiencia
- Evaluar la necesidad de realizar cambios en el SGSI
- Adecuar los objetivos y políticas en caso de que no cumplan con los requerimientos del SGSI

Para el cumplimiento de estos propósitos, las directivas de la institución se apoyaran en los resultados obtenidos en revisiones previas, retroalimentación por parte de los encargados de los procesos y la información, reportes sobre afectación y medidas de solución, recomendaciones de mejora impartidas por el comité SGSI.
Como resultado de la revisión y en caso de requerirse se generan acciones destinadas a:

- Mejorar la eficacia del SGSI
- Ajuste de Normas, políticas y procedimientos en respuesta a cambios internos o del entorno, requisitos del negocio, marco legal, criterios de aceptación de riesgos.
- Actualización de la evaluación de riesgos
- Actualización del plan de tratamiento de riesgos
- Requerimiento de nuevos recursos

Los resultados obtenidos en esta revisión deben ser consignados en un acta que será archivada en el archivo de la institución, serán puestos en conocimiento del comité SGSI quienes realizan seguimiento del cumplimiento de los acuerdos y cambios definidos.

B. MEJORA

Las directivas de la institución propenden por la mejora continua del SGSI, para lo cual gestionarán los recursos e insumos necesarios para este fin, para lo cual se apoyan en el resultado de la revisión, adicionalmente:

- Deben definir y establecer acciones y procedimientos correctivos tendientes a eliminar y garantizar que las causas que originen fallas al SGSI no vuelvan a ocurrir.
- Deben definir y establecer acciones y procedimientos preventivos con el fin de anticiparse a la aparición de acciones que puedan generar fallas en el SGSI y evitar su repetición.

Estas acciones deben ser debidamente documentadas y puestas a consideración del comité SGSI para su revisión, aprobación e implementación.

ANEXOS AL MANUAL SGSI DEL COLEGIO PRO-COLOMBIANO: POLITICAS

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Código	Col_ProCol_PSI
Versión:	0.1
Fecha de la versión	12/11/2016
Creado por:	Ing. Jerzon Álvarez
Aprobado por:	Junta directiva
Nivel de confidencialidad:	Alto

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
12/11/2016	0.1	Ing. Jerzon Álvarez	Descripción básica del documento

OBJETIVO, ALCANCE Y USUARIOS

El propósito de esta Política de alto nivel es definir el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información.

Esta Política se aplica a todo el Sistema de gestión de seguridad de la información (SGSI), según se define en el Documento del Alcance del SGSI.

Los usuarios de este documento son todos los empleados del **Colegio PRO-COLOMBIANO**, como también terceros externos a la institución.

1. Documentos de referencia

- Norma ISO/IEC 27001:2013, clausulas 5.2 y 6.2
- Documento sobre el alcance del SGSI
- Metodología de evaluación y tratamiento de riesgos
- Declaración de aplicabilidad
- Lista de obligaciones legales, normativas y contractuales
- [Política de la Continuidad del Negocio]
- [Procedimiento para gestión de incidentes]

Cumplimiento con la legislación con la legislación Colombiana:

- Ley 23 de 1982, derechos de autor.
- Ley 527 de 1999, comercio electrónico y firmas digitales.
- Ley 1273 de 2009, título de la protección de la Información y de los datos.
- Circular conjunta 01 de 2006, Orientaciones para el cumplimiento del derecho de autor y derechos conexos.

2. Terminología básica sobre seguridad de la información

Confidencialidad: característica de la información que está disponible solo para personas o sistemas autorizados.

Integridad: característica de la información que es modificada solo por personas o sistemas autorizados y de una forma permitida.

Disponibilidad: característica de la información a la cual pueden acceder solo las personas autorizadas cuando sea necesario.

Seguridad de la información: es la preservación de la confidencialidad, integridad y disponibilidad de la información.

Sistema de gestión de seguridad de la información: parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

POLÍTICA SOBRE DISPOSITIVOS MÓVILES

Código	Col_ProCol_PDM
Versión:	0.1
Fecha de la versión	12/11/2016
Creado por:	Ing. Jerzon Álvarez
Aprobado por:	Junta directiva
Nivel de confidencialidad:	Alto

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
12/11/2016	0.1	Ing. Jerzon Álvarez	Descripción básica del documento

1. Objetivo, alcance y usuarios

El objetivo del presente documento es evitar el acceso no autorizado a dispositivos ubicados tanto dentro como fuera de las instalaciones de la organización.

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todas las personas, datos y equipos incluidos en el alcance del SGSI.

Los usuarios de este documento son todos los empleados del **Colegio PRO-COLOMBIANO**.

Documentos de referencia

- Norma ISO/IEC 27001, clausulas A.6.2 y A.11.2.6
- Política de Seguridad de la Información
- [Política de Clasificación de la Información]
- [Política de Uso aceptable]

2. Computación móvil

2.1. Introducción

Entre los equipos de computación móvil se incluyen todo tipo de computadores, portátiles, teléfonos móviles, tarjetas de memoria y demás equipamiento móvil utilizado para almacenamiento, procesamiento y transferencia de datos.

El equipamiento mencionado anteriormente solamente puede ser transportado fuera de las instalaciones con la debida autorización de las directivas de la institución previa firma de un documento compromiso donde se garantice la confidencialidad de la información contenida en ellos.

La seguridad para estos equipos es equivalente a la que se realiza dentro de las instalaciones de la institución y se deben aplicar los siguientes controles adicionales, para mitigar los riesgos que por sí mismo conlleva el uso estos, así:

- Los equipos móviles institucionales, no pueden conectarse a redes inalámbricas públicas o no conocidas.
- El software instalado en los dispositivos móviles debe ser licenciado.
- El acceso a los equipos móviles se realiza mediante el uso de usuario y password.
- La información almacenada en los equipos de cómputo portátiles, debe ser cifrada.
- Se debe realizar borrado seguro de la información o destrucción física del dispositivo de almacenamiento, después de ser entregado por algún empleado que deje de pertenecer a la institución y antes de ser reasignado.
- Se debe realizar verificaciones periódicas para comprobar el retiro no autorizado de activos.

POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN

Código	Col_ProCol_PCI
Versión:	0.1
Fecha de la versión:	12/11/2016
Creado por:	Ing. Jerzon Álvarez
Aprobado por:	Junta directiva
Nivel de confidencialidad:	Alto

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
12/11/2016	0.1	Ing. Jerzon Álvarez	Descripción básica del documento

1. Objetivo, alcance y usuarios

El objetivo del presente documento es garantizar que se proteja la información en un nivel adecuado.

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todos los tipos de información, independientemente del formato, ya sean documentos en papel o electrónicos, aplicaciones y bases de datos, conocimiento de las personas.

Los usuarios de este documento son todos los empleados del **Colegio PRO-COLOMBIANO**.

2. Documentos de referencia

- Norma ISO/IEC 27001, clausulas A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.9.4.1, A.13.2.3
- Política de Seguridad de la Información
- Informe de evaluación y tratamiento de riesgos
- Declaración de aplicabilidad
- Inventario de activos
- Lista de obligaciones legales, normativas y contractuales
- Procedimiento para gestión de incidentes
- [Procedimientos operativos para tecnología de la información y de la comunicación] / [Política de eliminación y destrucción]
- Política de Uso aceptable

3. Información clasificada

3.1. Pasos y responsabilidades

Los pasos y responsabilidades para la gestión de la información son los siguientes:

Nombre del paso	Responsabilidad
1. Ingreso del activo de información en el Inventario de activos	[Definir responsable]
2. Clasificación de la información	Propietario del activo
3. Etiquetado de la información	Propietario del activo
4. Manejo de la información	Personas que poseen derechos de acceso de acuerdo con esta Política

Si la información clasificada proviene de afuera de la institución, el [definir responsable] es el responsable de su clasificación según las reglas establecidas en esta Política, y esta persona se convierte en el propietario de ese activo de información.

Clasificación de la información

La información se clasifica según su confidencialidad, integridad y disponibilidad de acuerdo con la sensibilidad e importancia de ésta.

Según su confidencialidad

La información se clasificará según su confidencialidad de la siguiente manera:

- **RESERVADO**: información cuya divulgación no autorizada puede ser perjudicial para los intereses o prestigio de la Institución.
- **INSTITUCIONAL**: información que debe ser conocida por los empleados de la institución para el desarrollo de sus actividades.
- **PUBLICA**: información de conocimiento público, entregada o divulgada sin restricciones.

Según su integridad

La información se clasificará según su integridad de la siguiente manera:

4. No puede repararse y ocasiona pérdidas graves para la institución.
3. Difícil reparación y produce pérdidas significativas.
2. Puede repararse, produce pérdidas leves.
1. No afecta la operación y puede repararse fácilmente.

Según su disponibilidad

La información se clasificará según su disponibilidad de la siguiente manera:

Es necesario determinar el tiempo máximo tolerable MTD de indisponibilidad que puede soportar la institución sin un activo determinado, para lo cual se tendrá en cuenta la siguiente clasificación:

5. **CRÍTICOS**, la interrupción es de minutos y hasta 12 horas.
4. **URGENTE**, la interrupción hasta por 24 horas.
3. **IMPORTANTE**, interrupción hasta por 72 horas.
2. **NORMAL**, interrupción de hasta siete días
1. **NO ESENCIALES**, la interrupción es de hasta 30 días

POLÍTICA DE USO ACEPTABLE

Código	Col_ProCol_PUA
Versión:	0.1
Fecha de la versión:	12/11/2016
Creado por:	Ing. Jerzon Álvarez
Aprobado por:	Junta directiva
Nivel de confidencialidad:	Alto

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
12/11/2016	0.1	Ing. Jerzon Álvarez	Descripción básica del documento

1. Objetivo, alcance y usuarios

El objetivo del presente documento es definir reglas claras para el uso de los sistemas y de otros activos de información en el **Colegio PRO-COLOMBIANO**.

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todos los sistemas y demás activos de información utilizados dentro del alcance del SGSI.

Los usuarios de este documento son todos los empleados del **Colegio PRO-COLOMBIANO**.

2. Documentos de referencia

- Norma ISO/IEC 27001, clausulas A.6.2.1, A.6.2.2, A.8.1.2, A.8.1.3, A.8.1.4, A.9.3.1, A.11.2.5, A.11.2.6, A.11.2.8, A.11.2.9, A.12.2.1, A.12.3.1, A.12.5.1, A.12.6.2, A.13.2.3, A.18.1.2
- Política de Seguridad de la Información
- [Política de Clasificación de la Información]
- [Procedimiento para gestión de incidentes]
- [Inventario de activos]
- [Procedimientos operativos para tecnología de la información y de la comunicación]
- [Política de Transferencia de la Información]

3. Uso aceptable de los activos de información

3.1. Definiciones

Sistema de información: incluye todos los servidores y clientes, infraestructura de red, software del sistema y aplicaciones, datos y demás subsistemas y componentes que pertenecen o son utilizados por la institución, o que se encuentran bajo su responsabilidad. El uso de un sistema de información también incluye el uso de todos los servicios internos o externos, como el acceso a Internet, correo electrónico, etc.

Activos de información: en el contexto de esta Política, el término activos de información se aplica a los sistemas de información y demás información o equipos, incluyendo documentos en papel, teléfonos móviles, computadores portátiles, soportes de almacenamiento de datos, etc.

POLÍTICA DE CLAVES

Código	Col_ProCol_PC
Versión:	0.1
Fecha de la versión:	12/11/2016
Creado por:	Ing. Jerzon Álvarez
Aprobado por:	Junta directiva
Nivel de confidencialidad:	Alto

Historial de modificaciones

Fecha	**Versión**	**Creado por**	**Descripción de la modificación**
12/11/2016	0.1	Ing. Jerzon Álvarez	Descripción básica del documento

1. Objetivo, alcance y usuarios

El objetivo del presente documento es establecer reglas para garantizar la gestión y utilización seguras de las claves.

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todos los puestos de trabajo y sistemas ubicados dentro del alcance del SGSI.

Los usuarios de este documento son todos los empleados del **Colegio PRO-COLOMBIANO**.

2. Documentos de referencia

- Norma ISO/IEC 27001, clausulas A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3
- Política de Seguridad de la Información
- Declaración de aceptación de los documentos del SGSI

3. Obligaciones de los usuarios

Los usuarios deben aplicar buenas prácticas de seguridad en cuanto a la elección y uso de claves:

POLÍTICA DE CONTROL DE ACCESO

Código	Col__ProCol_PCA	
Versión:	0.1	
Fecha de la versión:	12/11/2016	
Creado por:	Ing. Jerzon Álvarez	
Aprobado por:	Junta Directiva	
Nivel de confidencialidad:	Alto	

Historial de modificaciones

Fecha	**Versión**	**Creado por**	**Descripción de la modificación**
12/11/2016	0.1	Ing. Jerzon Álvarez	Descripción básica del documento

1. Objetivo, alcance y usuarios

El objetivo del presente documento es definir reglas de acceso para diversos sistemas, equipos, instalaciones e información en base a los requerimientos de negocios y de seguridad.

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todos los sistemas, equipos, instalaciones e información utilizados dentro del alcance del SGSI.

Los usuarios de este documento son todos los empleados del **Colegio PRO-COLOMBIANO**.

2. Documentos de referencia

- Norma ISO/IEC 27001, clausulas A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.3
- Política de Seguridad de la Información
- Declaración de aplicabilidad
- [Política de Clasificación de la Información]
- [Declaración de aceptación de los documentos del SGSI]
- [Lista de requisitos legales, normativos, contractuales y de otra índole]

3. Control de acceso

3.1. Introducción

El principio básico es que el acceso a todos los sistemas, redes, servicios e información está prohibido salvo que sea expresamente permitido a usuarios individuales o a grupos de usuarios. Debe existir un procedimiento de registro de usuarios para cada sistema y servicio.

Está permitido el acceso a todos los sectores físicos de la institución excepto a aquellos para las cuales el privilegio debe ser concedido por una persona autorizada.

Esta Política determina.

Todo empleado de la institución con acceso a Internet a través del servicio contratado por la institución, tiene restringido el uso de:

- Mensajería instantánea comercial.
- La telefonía a través de internet.
- Correo electrónico comercial no autorizado.
- Descarga de archivos de sitio peer to peer.
- Conexiones a sitios de streaming no autorizado.
- Acceso a sitios de pornografía.
- Servicios de escritorio remoto a través de internet.
- Cualquier otro servicio que vulnere la seguridad de la red o degrade el desempeño de la misma.

POLÍTICA DE ELIMINACIÓN Y DESTRUCCIÓN

Código	Col_ProCol_PEyD
Versión:	0.1
Fecha de la versión:	12/11/2016
Creado por:	Ing. Jerzon Álvarez
Aprobado por:	Junta Directiva
Nivel de confidencialidad:	Alto

Historial de modificaciones

Fecha	**Versión**	**Creado por**	**Descripción de la modificación**
12/11/2016	0.1	Ing. Jerzon Álvarez	Descripción básica del documento

1. Objetivo, alcance y usuarios

El objetivo del presente documento es garantizar que la información almacenada en equipos y soportes sea borrada o eliminada de forma segura.

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a toda la tecnología de la información y de la comunicación, como también a la documentación dentro del alcance del SGSI.

Los usuarios de este documento son todos los empleados del **Colegio PRO-COLOMBIANO**.

2. Documentos de referencia

- Norma ISO/IEC 27001, clausulas A.8.3.2, A.11.2.7
- Política de Seguridad de la Información
- [Política de Clasificación de la Información]
- [Inventario de activos]

3. Eliminación y destrucción de equipos y soportes

Todos los datos y software con licencia almacenados en soportes móviles (por ej., CD, DVD, unidades USB, tarjetas de memoria, discos duros., y también en papel) y en todos los equipos que tienen soportes de almacenaje (por ej., computadores tanto de mesa y portátiles, teléfonos móviles, etc.) deben ser borrados, o se debe destruir el soporte, antes de su devolución o reutilización.

POLÍTICA DE PANTALLA Y ESCRITORIO LIMPIOS

Código	Col_ProCol_PyEL
Versión:	0.1
Fecha de la versión:	12/11/2016
Creado por:	Ing. Jerzon Álvarez
Aprobado por:	Junta Directiva
Nivel de confidencialidad:	Alto

Historial de modificaciones

Fecha	**Versión**	**Creado por**	**Descripción de la modificación**
12/11/2016	0.1	Ing. Jerzon Álvarez	Descripción básica del documento

1. Objetivo, alcance y usuarios

El objetivo del presente documento es definir reglas para evitar el acceso no autorizado a la información en los puestos de trabajo, como también a las instalaciones y a los equipos compartidos.

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todos los puestos de trabajo, instalaciones y equipos ubicados dentro del alcance del SGSI.

Los usuarios de este documento son todos los empleados del **colegio PRO-COLOMBIANO**

2. Documentos de referencia

- Norma ISO/IEC 27001, clausulas A.11.2.8 y A.11.2.9
- Política de Seguridad de la Información
- [Política de Clasificación de la Información]

3. Política de pantalla y escritorio limpio

Toda la información clasificada como "Uso interno", "Restringido" y "Confidencial" de acuerdo a lo establecido en la Política de Clasificación de la Información, es considerada sensible en esta Política de pantalla y escritorio limpio.

3.1. Protección del puesto de trabajo

3.1.1. Política de escritorio limpio

- Si la persona autorizada no se encuentra en su puesto de trabajo, todos los documentos impresos, como también los soportes de almacenamiento de datos deben estar almacenados en sitios seguros bajo llave, especialmente si la persona se encuentra fuera de su horario laboral.
- Cuando el empleado no se encuentre utilizando el computador, debe bloquearse la sesión, el protector de pantalla se debe activar automáticamente después de cinco (5) minutos de inactividad.
- Cuando se imprima información considerada como sensible no se debe dejar disponible, debe ser almacenada inmediatamente.

PROCEDIMIENTOS PARA TRABAJO EN ÁREAS SEGURAS

Código	Col_ProCol_TAS
Versión:	0.1
Fecha de la versión:	12/11/2016
Creado por:	Ing. Jerzon Álvarez
Aprobado por:	Junta directiva
Nivel de confidencialidad:	Alto

Historial de modificaciones

Fecha	**Versión**	**Creado por**	**Descripción de la modificación**
12/11/2016	0.1	Ing. Jerzon Álvarez	Descripción básica del documento

1. Objetivo, alcance y usuarios

El objetivo de este documento es definir las reglas básicas de comportamiento en las áreas seguras.

Este documento se aplica a todas las áreas seguras del Sistema de gestión de seguridad de la información (SGSI).

Los usuarios de este documento son todos los empleados del **colegio PRO-COLOMBIANO**

2. Documentos de referencia

- Norma ISO/IEC 27001, clausulas A.11.1.5
- Política de control de acceso
- Inventario de activos

3. Reglas para áreas seguras

3.1. Lista de áreas seguras

Las áreas seguras existentes que requieren reglas especiales son las siguientes:

- Sala de informática
- Sala de archivos
- Almacenamiento de equipos
- Oficinas

Las personas responsables para cada área segura se detallan como propietarios de activos en el Inventario de activos.

3.2. Derecho de acceso a áreas seguras

El acceso a las áreas seguras se autoriza de acuerdo con la Política de control de acceso.

POLÍTICA DE TRANSFERENCIA DE LA INFORMACIÓN

Código:	Col_ProCol_TDI
Versión:	0.1
Fecha de la versión:	12/11/2016
Creado por:	Ing. Jerzon Álvarez
Aprobado por:	Junta Directiva
Nivel de confidencialidad:	Alto

Historial de modificaciones

Fecha	**Versión**	**Creado por**	**Descripción de la modificación**
12/11/2016	0.1	Ing. Jerzon Álvarez	Descripción básica del documento

1. Objetivo, alcance y usuarios

El objetivo del presente documento es asegurar la seguridad de la información y el software cuando son intercambiados dentro o fuera de la organización.

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a toda la información y tecnología de la información y de la comunicación utilizada dentro del alcance del SGSI.

Los usuarios de este documento son empleados de colegio PRO-COLOMBIANO

2. Documentos de referencia

- Norma ISO/IEC 27001, puntos A.13.2.1, A.13.2.2
- Política de Seguridad de la Información
- [Política de Clasificación de la Información]
- [Política de seguridad para proveedores]

3. Transferencia de la información

3.1. Canales de comunicación electrónica

La información de la organización puede ser intercambiada a través de los siguientes canales de comunicación electrónica: correo electrónico, descarga de archivos desde Internet, transferencia de datos por medio de [Dropbox, OneDrive], teléfonos, equipos de fax, mensajes de texto por teléfonos móviles, soportes móviles y foros o redes sociales.

Apéndice: Registro de incidentes

Los incidentes tales como: fallas humanas (voluntarias e involuntarias), ataques informáticos, errores del sistema, desastres naturales, fallas de sistemas de alimentación, se clasifican dentro de los siguientes tipos:

- Relacionados con la información (directamente relacionados con tecnología de la información y comunicación)
- No relacionados con la información (todos los demás incidentes)

PROCEDIMIENTO PARA GESTIÓN DE INCIDENTES DE SEGURIDAD

Código	Col_ProCol_GIS
Versión:	0.1
Fecha de la versión:	12/11/2016
Creado por:	Ing. Jerzon Álvarez
Aprobado por:	Junta Directiva
Nivel de confidencialidad:	Alto

Historial de modificaciones

Fecha	**Versión**	**Creado por**	**Descripción de la modificación**
12/11/2016	0.1	Ing. Jerzon Álvarez	Descripción básica del documento

1. Objetivo, alcance y usuarios

El objetivo del presente documento es garantizar la detección temprana de eventos y debilidades de seguridad, como también la rápida reacción y respuesta ante incidentes de seguridad.

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todos los empleados y demás activos que se utilizan dentro del alcance del SGSI, como también a los proveedores y demás personas externas a la organización que entran en contacto con los sistemas y con la información alcanzados por el SGSI.

Los usuarios de este documento son todos los empleados del **colegio PRO-COLOMBIANO**, como también las personas mencionadas precedentemente.

2. Documentos de referencia

- Norma ISO/IEC 27001, clausulas A.7.2.3, A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
- Política de Seguridad de la Información
- [Lista de requisitos legales, normativos, contractuales y de otra índole]

3. Gestión de incidentes

Un incidente de seguridad de la información es un "evento, o serie de eventos, indeseado e inesperado que tiene una alta probabilidad de poner en riesgo las actividades comerciales y de amenazar la seguridad de la información" (ISO/IEC 27000:2009).

3.1. Recepción y clasificación de incidentes, debilidades y eventos

Cada empleado, proveedor o tercero que esté en contacto con información y/o sistemas de información debe reportar de la siguiente manera toda debilidad del sistema, incidente o evento que pudiera derivar en un posible incidente:

- Reportar los eventos de seguridad siguiendo los procedimientos operativos establecidos para tal fin.
- Informar de forma completa e inmediata la existencia de un potencial incidente de seguridad informática que afecte a activos de información considerado como crítico.
- Ejecutar acciones tendientes a reducir y mitigar el incidente.
- Asimilar de las experiencias tenidas ende los incidentes de seguridad de la información, para aprender a prevenir nuevas ocurrencias.
- Subsanar las consecuencias de los incidentes de seguridad de la información.