Vulnerabilidad en plataformas virtuales y redes sociales en estudiantes de educación media del municipio de Pasto: Estudio de Caso Institución Educativa Municipal Ciudad de Pasto año 2023

Autores

David Sebastián Martínez Delgado

Camilo Andrés Bravo Rosero

Universidad Mariana

Facultad de Ingeniería

Programa de Ingeniería de Sistemas

San Juan de Pasto

2024

Vulnerabilidad en plataformas virtuales y redes sociales en estudiantes de educación media del municipio de Pasto: Estudio de Caso Institución Educativa Municipal Ciudad de Pasto año 2023.

Autores(s)

David Sebastián Martínez Delgado

Camilo Andrés Bravo Rosero

Trabajo de grado como requisito para obtener el título de Ingeniero de Sistemas

José Javier Villalba Romero

Asesor

Universidad Mariana

Facultad de Ingeniería

Programa de Ingeniería de Sistemas

San Juan de Pasto

2024

ARTÍCULO 71

REGLAMENTO DE INVESTIGACIONES

UNIVERSIDAD MARIANA

"Los conceptos, afirmaciones y opiniones emitidos en el Trabajo de Grado son responsabilidad única y exclusiva del (los) Educando (s). "

NOTA DE ACEPTACIÓN:

_____

_____

_____

_____

_____

_____

_____

Firma presidente del jurado

_____

Firma del Jurado

_____

Firma del Jurado

Dedicatoria

A nuestros padres, por su amor incondicional, por creer siempre en nosotros y por ser nuestro pilar fundamental en todo momento.

A nuestras familias, por su apoyo constante y por brindarnos la fortaleza necesaria para alcanzar nuestras metas.

A mi madre que estuvo en toda mi carrera y me apoyo moral y económicamente para que no me faltara nada.

A nuestros amigos, por su compañía y motivación, y por ser una fuente constante de ánimo y alegría.

A todos aquellos que han sido parte de este camino, por su paciencia, comprensión y por ayudarnos a superar cada obstáculo.

Dedicamos este proyecto a todas las personas que creen en la educación y en el poder transformador del conocimiento, con la esperanza de contribuir a un futuro más seguro y consciente en el uso de las redes sociales.

Camilo Andrés Bravo Rosero

Agradecimientos

La culminación de este proyecto de grado sobre "Vulnerabilidad en plataformas virtuales y redes sociales en estudiantes de educación media del municipio de Pasto en los años 2022 y 2023" no habría sido posible sin la colaboración y el apoyo de muchas personas e instituciones a quienes quiero expresar mi más profundo agradecimiento.

En primer lugar, Agradecemos a los profesores del Departamento de Ingeniería de Sistemas de la Universidad Mariana por su dedicación y enseñanza, que han enriquecido nuestra formación académica y profesional.

Queremos agradecer a nuestro asesor, el Dr. José Javier Villalba Romero, por su apoyo, orientación a lo largo de todo este proceso. Por sus sugerencias y comentarios han sido esenciales para la realización de este trabajo.

Nuestro más sincero agradecimiento a la Universidad Mariana y a sus autoridades por brindar los recursos necesarios y el entorno adecuado para la realización de esta investigación. Agradecemos también al personal administrativo por su amabilidad y colaboración en todo momento.

Queremos expresar nuestra gratitud a la Institución Educativa Municipal Ciudad de Pasto por su apoyo y por permitirnos llevar a cabo este estudio en sus instalaciones.

En el ámbito personal, queremos agradecer profundamente a nuestras familias, especialmente a nuestros padres, por su amor, apoyo incondicional y por siempre creer en nosotros. A nuestros amigos por su compañía y ánimos constantes durante estos años.

Tabla de Contenido

1 Elementos del Proceso Investigativo 15
1.1 Antecedentes y Estado del Conocimiento 15
1.2 Titulo 17
1.3. Problema de Investigación 18
1.3.1 Descripción del problema 18
1.3.2 Formulación del problema 19
1.4 Objetivos 19
1.4.1 Objetivo general 19
1.4.2 Objetivos Específicos 19
1.5 Justificación 19
1.6 Marcos de Referencia 20
1.6.1 Marco Teórico – Conceptual 20
1.7 Metodología 26
1.7.1 Paradigma, enfoque y tipo de investigación 26
1.7.2 Línea y Áreas Temáticas de investigación 27
1.7.3 Población y muestra 27
1.7.4 Proceso de investigación 28
1.7.5 Variables e hipótesis 29
1.8 Presupuesto 31
1.9 Cronograma 33
1.10 Productos Esperados 34
2. Desarrollo del Proceso Investigativo 35
2.1 Información y Recursos Informáticos de la IEM Ciudad de Pasto 35
2.2 Identificación de Activos 41
2.2.1 Inventario de activos informáticos del área administrativa de la IEM Ciudad de Pasto 43
2.2.2 Inventarios de activos informáticos del área informática de la IEM Ciudad de Pasto 44
2.2.3 Inventario de activos informáticos del área académica de la IEM Ciudad de Pasto 45

2.2.4 Inventario de activos informáticos del área de convivencia de la IEM Ciudad de Pasto.....46
2.3 Descripción del Área de Rectoría de la IEM Ciudad de Pasto.....46
2.3.1 Descripción del área de coordinación académica y de convivencia de la IEM Ciudad de Pasto 47
2.3.2 Descripción de las aulas informáticas de la IEM Ciudad de Pasto 49
2.3.4 Evidencias Fotográficas de los recursos informáticos en la IEM Ciudad de Pasto 51
2.3.5 Evidencia fotográfica aulas de Informática 51
2.4 Vulnerabilidades, Riesgos y Amenazas en la IEM Ciudad de Pasto 59
2.4.1 Matrices de riesgos y amenazas Magerit 80
2.4.2 Valoración de activos mediante la norma ISO/IEC 27001 87
2.4.3 Identificación de amenazas en la institución 94
2.4.4. Diseño del plan para gestionar riesgos mediante el uso de las directrices de calidad establecida en la norma ISO/IEC 27001 95
2.5. Guía para la implementación de la ISO /IEC 27001 en la IEM San Juan de Pasto.....96
Conclusiones.....111
Recomendaciones.....113
Referencias bibliográficas 115

Lista de Tablas

Tabla 1 *Proceso de investigación* 28
Tabla 2 *Variables* 29
Tabla 3 *Presupuesto global del proyecto* 31
Tabla 4 *Descripción de la Inversión en personal.* 31
Tabla 5 *Presupuesto de materiales y equipos.* 31
Tabla 6 *Cronograma* 33
Tabla 7 *Inventario de activos informáticos de la IEM Ciudad de Pasto (Área administrativa)* 43
Tabla 8 *Inventario de activos informáticos de la IEM Ciudad de Pasto (Área informática)* 44
Tabla 9 *Inventario de activos informáticos de la IEM Ciudad de Pasto (Área académica)* 45
Tabla 10 *Inventario de activos informáticos de la IEM Ciudad de Pasto (Área convivencia)* 46
Tabla 11 *Descripción área de rectoría IEM Ciudad de Pasto* 47
Tabla 12 *Descripción área de coordinación académica y de convivencia IEM Ciudad de Pasto* 48
Tabla 13 *Descripción aulas de informática IEM Ciudad de Pasto* 49
Tabla 14 *Clasificación del riesgo* 81
Tabla 15 *Matriz de evaluación de seguridad informática* 82
Tabla 16 *Matriz de amenazas por redes sociales* 82
Tabla 17 *Matriz de conocimiento de casos de ciberataques* 83
Tabla 18 *Matriz de delitos informáticos en la institución* 85
Tabla 19 *Delitos informáticos con mayor incidencia.* 86
Tabla 20 *Evaluación de activos por propiedades* 88
Tabla 21 *Clasificación de activos* 89
Tabla 22 *Valoración de activos en la institución* 90
Tabla 23 *Propiedades de los activos* 91
Tabla 24 *Identificación de amenazas con Magerit.* 94
Tabla 25 *Controles de dominios de la norma ISO/IEC 2700* 102

Listas de Figuras

Figura 1 *Diagrama de flujo de gestión Directiva.* 36
Figura 2 *Diagrama de flujo de gestión académica* 38
Figura 3 *Diagrama de flujo de gestión administrativa y financiera.* 39
Figura 4 *Diagrama de flujo de la gestión comunitaria* 40
Figura 5 *Grados encuestados* 60
Figura 6 *Edades encuestadas* 61
Figura 7 *Géneros Encuestados* 61
Figura 8 *Roles* 62
Figura 9 *Distribución del Uso de Dispositivos Tecnológicos* 63
Figura 10 *Frecuencia uso de Redes sociales* 63
Figura 11 *Nivel de Información de los Usuarios* 64
Figura 12 *Experiencias de Vulnerabilidad en Redes Sociales* 65
Figura 13 *Vulnerabilidades más frecuentes* 65
Figura 14 *Antivirus en aulas de informática* 66
Figura 15 *Antivirus actualizados* 67
Figura 16 *Conocimientos de delitos informáticos* 67
Figura 17 *Seguridad de la información* 68
Figura 18 *Conocimiento de vulnerabilidades de seguridad* 69
Figura 19 *Capacitación de la Institución* 69
Figura 20 *Conocimiento de plataformas virtuales* 70
Figura 21 *Frecuencia en redes sociales* 70
Figura 22 *Medidas de protección en redes sociales* 71
Figura 23 *Información personal compartida* 71
Figura 24 *Conocimiento de políticas de seguridad informática* 72
Figura 25 *Casos de vulnerabilidades* 72
Figura 26 *Interacciones en redes sociales* 73
Figura 27 *Intervención Institucional en Casos de Vulnerabilidad* 74
Figura 28 *Promueve el uso responsable de redes sociales* 74
Figura 29 *Orientación y recursos* 75
Figura 30 *Prevención de situaciones de vulnerabilidad* 75

Figura 31 *Denuncia de situaciones de vulnerabilidad* 76
Figura 32 *Conocimiento de medidas de seguridad* 76
Figura 33 *Interacción con personas desconocidas* 77
Figura 34 *Aumento en el acoso en línea* 77
Figura 35 *Situaciones de denuncias* 78
Figura 36 *Educación sobre seguridad* 78
Figura 37 *Contenido compartido en redes sociales* 79

Listas de Imágenes

Imagen No. 1 Aula informática # 1 51
Imagen No. 2 Aula informática # 1 52
Imagen No. 3 Aula informática # 1 52
Imagen No. 4 Aula informática # 2 53
Imagen No. 5 Aula informática # 2 54
Imagen No. 6 Aula informática # 3 55
Imagen No. 7 Aula informática # 3 55
Imagen No. 8 Aula informática Galileo 56
Imagen No. 9 Aula informática Galileo 57
Imagen No. 10 Oficina de Ingeniería y recursos tecnológicos 58
Imagen No. 11 Oficina de Ingeniería y recursos tecnológicos. 59

Listas de Anexos

Anexo 1 Aval de institucional 117

Anexo 2 Formularios de encuesta 118

Introducción

La vulnerabilidad de los jóvenes en las redes sociales cada vez es mayor, sobre todo si no se logra generar una adecuada educación y prevención de los delitos virtuales, en donde, los niños, niñas y adolescentes se pueden ver involucrados en nuevas maneras de acoso y ciberbullying como lo son: Mensajes obscenos, sexting, Grooming, sextorsión, pornografía infantil, entre otros, generando mayores inseguridades y peligros a la hora de tener una conexión segura a las plataformas digitales sobre todo en una época en la cual la virtualidad ha sido el eje central de lo cotidiano. Ante este panorama se pretende realizar una investigación que permita determinar el grado de vulnerabilidad informática y riesgos de los jóvenes estudiantes de la institución educativa ciudad de Pasto, analizando y comprendiendo la situación y panorama actual, teniendo como referente la implementación de la educación mediante la virtualidad.

Este estudio se realizó con los estudiantes de grado decimo y once de la Institución Educativa Municipal ciudad de Pasto en el año 2023, con el fin de permitirle a la institución y sus estudiantes identificar las vulnerabilidades ocurridas dentro de los procesos virtuales tanto académicos como personales y poder implementar planes de mejoramiento que conduzcan a fortalecer la seguridad informática con buenas prácticas en el uso de herramientas tecnológicas por parte de la comunidad educativa. Se realizó mediante encuestas y charlas que permitan entrar en confianza con los actores e implantar metodologías de seguridad de la información en este caso MAGERIT que es la metodología usada para conocer los riesgos a los que se enfrenta un sistema y poder implementar las medidas necesarias para mitigar esos riesgos, facilitando a implementación de esquemas de seguridad informática e ISO/IEC 27001 que es una norma internacional que describe cómo gestionar la seguridad de la información en una organización, es la primera norma a nivel mundial de la seguridad de la información y se puede certificar, esta norma busca proteger los datos que almacena una organización, el paso inicial para su implementación es el estudio de riesgos y con sus resultados se realiza un análisis e implementación de actividades para proteger los datos, generando una mitigación de riesgos.

1 Elementos del Proceso Investigativo

1.1 Antecedentes y Estado del Conocimiento

Las redes sociales actualmente son un epicentro de información, en el cual se puede encontrar una gran propagación de malware, centradas en buscar credenciales para generar ataques generalmente con el fin de obtener información personal en ocasiones para beneficio netamente monetario, aunque también se hace para crear sabotajes en contra de la integridad de la persona afectada, hablando de ciberseguridad, Adriana Ceballos, directora de TicTac afirma que "la ciberseguridad es el área que mayor atención deberá tener en el 2021, pues un gran número de colaboradores seguirán operando desde sus hogares" además según las cifras de la Fiscalía General de la Nación los ciberataques entre marzo y noviembre del anterior año tuvieron un incremento superior al 98% y la suplantación de identidades en sitios web tuvo un incremento en denuncia del 372% en comparación con el año 2019. (Henao, 2020)

Con el fin de abordar más el tema de las redes sociales en adolescentes se toma como referencia la investigación realizada por un grupo de estudiantes, la cual se denominó "*Investigación aplicada: influencia del uso de redes sociales en los síntomas de ansiedad en jóvenes entre los 12 y los 18 años de edad en el colegio I.E María Cano*" (Rengifo, 2020 p 3) se afirma que la vulnerabilidad en estudiantes entre los 12 a 18 años de edad es muy grande ya que pasan demasiado tiempo en redes sociales, generando en los niños y adolescentes síntomas graves de ansiedad por el uso sin límite alguno de los medios de comunicación virtual, cabe aclarar que el estudio por falta de tiempo carece de aspectos analíticos donde se determine si la ansiedad es el factor número uno en vulnerabilidad o hay aspectos secundarios.

El ámbito familiar contribuye mucho a la educación y la responsabilidad cibernética, la educación brindada en casa y las enseñanzas siempre van de la mano con aspectos como la obsesión por los medios de comunicación virtuales como lo son las redes sociales, según una investigación hecha por un estudiante de psicología afirma que "*se indica la existencia de una correlación directamente proporcional entre el funcionamiento familiar y la adicción a las redes sociales"* (Pinto, 2018 p 20) este estudio da las bases para entender que la unidad familiar es de gran ayuda

en el área de la vida social en la virtualidad. Relacionando la psicología, el rol en las redes sociales y como unidad de análisis la estadística.

Actualmente los jóvenes pasan demasiado tiempo en el internet y las redes sociales, además un alto número de jóvenes se ve expuesto y se siente vulnerable en estos medios de información masiva, según una investigación realizada por estudiantes de trabajo social en su texto denominado "Menores y redes sociales: riesgo de un mal uso" afirman que *"Un alto número de menores han indicado que consideran que han sido víctimas de acoso escolar, que han recibido empujones, insultos, que les han quitado sus pertenencias, llegado a excluir de un grupo, hasta incluso, recibir amenazas por parte de otros/as compañeros/as. Considerando, también, que estas acciones se han visto acentuadas a través de las redes sociales. Son datos alarmantes que ponen en manifiesto que muchos/as menores a pesar de la información recibida al respecto, siguen promoviendo conductas vejatorias a sus compañeros/as. El simple hechos de estar en red hace que los/as menores estén más expuestos/as al riesgo. Siendo pocos/as los/as que son conscientes de que el uso que hacen de internet puede generar aspectos negativos para sí mismos/as, puesto que a pesar de considerar que sí lo son, sus acciones determinan lo contrario. Son muchos/as los/as encuestados/as que han indicado que mantienen contacto con personas desconocidas, recibiendo y enviando imágenes, llegando incluso a conocerse personalmente, lo que deja en evidencia que no son conscientes del riesgo al que se exponen, como puede ser una persona con una identidad falsa."* (Gonzales & Hernández, 2017, p. 39) Esto confirma lo que se viene exponiendo a lo largo del documento, los estudiantes y jóvenes día con día se ven expuestos y son vulnerables ante las redes sociales ya que se exponen a un mundo que creen conocer, pero puede ser un espacio totalmente desconocido para ellos.

Los adolescentes cuentan con un gran interés por el uso de los recursos virtuales, no sólo en lo relacionado con la comunicación, sino para hacer búsquedas de información y creación de contenidos que los identifique frente al mundo y a la vida. Desde esta perspectiva, las instituciones educativas y las familias, deben profundizar en temas de actualización tecnológica, en cuanto al conocimiento de lo que son en realidad las redes virtuales, con el fin de evitar el rezago ante el avance social, ahora también virtual, y si evitar todo tipo de ataques cibernéticos. Uno de los principales peligros conocidos en las redes sociales con respecto a los estudiantes es el ciberbullying, en donde, con el uso de las nuevas tecnologías de información y comunicación se

han presentado vulneraciones y amenazas a los jóvenes. Por lo anterior, es muy común que los estudiantes sean vulnerables entre si ya que son capaces de realizar matoneo por redes sociales y plataformas digitales sin saber que tanto daño le están realizando a la otra persona, esto se debe a la falta de educación sobre el buen uso de redes sociales y plataformas digitales.

Según las referencias anteriores sobre el tema a trabajar se puede observar que es muy recurrente la vulnerabilidad que existe en redes sociales mediante el uso de las tecnologías de comunicación, pero que a la vez por falta de conocimiento se permite de manera inconsciente el ingreso de malware a los equipos y con ello vulneración a datos personales. Con la revisión de los antecedentes, se encuentra que existen diferentes formas de vulnerabilidad en redes sociales, lo cual genera en los jóvenes desde principios de ansiedad hasta el fomento del ciberbullying. Como se escribió anteriormente se observa el incremento en la inseguridad cibernética, la dependencia de los jóvenes a las redes sociales y los lazos familiares son unas de las posibles causas de estas vulnerabilidades la situación socioeconómica y su salud mental.

Los antecedentes mencionadas brindan un panorama para poder abordar el presente trabajo investigativo de la manera más completa y eficaz, conociendo aspectos importantes como ciberseguridad, delitos informáticos, nuevas modalidades de matoneo dentro de las redes y plataformas educativas y los riesgos que estos traen no solo para la integridad física sino psicológica de los estudiantes y sus familias, factores muy importantes a la hora de evaluar la vulnerabilidad a la que los jóvenes se enfrentan en la cotidianidad de la virtualidad. Logrando realizar una investigación completa en todas las áreas en las que influye la vulnerabilidad en la seguridad de los jóvenes estudiantes.

1.2 Titulo

Vulnerabilidad en plataformas virtuales y redes sociales en estudiantes de educación media del municipio de Pasto: Estudio de Caso Institución Educativa Municipal Ciudad de Pasto año 2023.

1.3. Problema de Investigación

1.3.1 Descripción del problema

La vulnerabilidad en redes sociales es muy común en el momento y más si se habla de personas en etapa de niñez y adolescencia, los índices de cibercrimenes en Colombia han venido creciendo según el informe de Cisco 2019-2020, esta situación genera preocupación ya que desencadena desconfianza y zozobra en las personas y en las organizaciones. El informe muestra la violación de datos personales que se registraron para el año 2019-2020 fue de 8.037 casos, según la cifra de este delito se lo considera como la segunda amenaza de cibercrimenes en Colombia, donde se puede observar que los delitos informáticos son unas de los principales problemas de ciberseguridad que se está afrontando actualmente en Colombia. (Cisco, 2020, p 6-7)

El aislamiento obligatorio y la cuarentena declarada por el gobierno en el mes de marzo de 2020 ha hecho que muchas de las actividades que antes se hacían de manera presencial ahora se realicen usando plataformas virtuales. La educación no ha sido ajena a esto y muchos colegios e instituciones educativas se vieron obligadas a seguir sus clases mediante el uso de plataformas virtuales y redes sociales, lo cual ha generado muchos inconvenientes entre los que se destacan algunos ataques y vulnerabilidades a sus sistemas informáticos, “Para el mes de noviembre de 2020 se encuentra un aumento del 83% de delitos cometidos en épocas de pandemia con respecto al 2019, más concretamente hubieron 21.107 casos mientras que en 2020 aumento 36.834 delitos informáticos” (Acosta, 2022).

Por lo anteriormente expuesto, el sector educativo en Colombia está en terreno desconocido frente a la virtualidad, motivo por el cual se busca indagar sobre esta problemática y el impacto que ha causado en los jóvenes el uso de estas mediaciones tecnológicas en sus procesos educativos, ya que con ello se podrán implementar medidas que aporten a mejorar la seguridad ante vulnerabilidades por ataques informáticos en las tecnologías usadas para su proceso pedagógico.

1.3.2 Formulación del problema

¿Cómo evaluar la vulnerabilidad informática en plataformas virtuales y redes sociales en los estudiantes de grado once y decimo en la Institución Educativa Municipal Ciudad de Pasto del Municipio de Pasto?

1.4 Objetivos

1.4.1 Objetivo general

Analizar la vulnerabilidad informática en plataformas digitales y redes sociales en los estudiantes de grado decimo y once de la Institución Educativa Municipal Ciudad de Pasto del municipio de Pasto bajo el estándar MAGERIT e ISO/IEC 27001para el año 2023.

1.4.2 Objetivos Específicos

- Identificar la información y los recursos informáticos que maneja la IEM Ciudad de Pasto en sus procesos educativos.
- Determinar vulnerabilidades, riesgos y amenazas en medios informáticos usados para la virtualidad en el proceso pedagógico en grados decimo y once de la institución objeto de estudio, bajo metodología Magerit e ISO/IEC 27001
- Diseñar una propuesta para el mejoramiento de la seguridad informática en la institución educativa objeto de estudio.

1.5 Justificación

La vulnerabilidad en las redes sociales y en la juventud actualmente es muy común se puede ver que día a día se vive en una realidad que cada vez es más virtual. Con esta investigación se busca identificar los focos de vulnerabilidades y el peligro que pueden correr los jóvenes estudiantes en las redes sociales y plataformas virtuales. Llevando como centro de la investigación el ¿por qué? Estas plataformas se han vuelto un epicentro de ataques virtuales a estudiantes y cuál es la motivación principal de los agresores y como los jóvenes responden a estos ataques. Se busca analizar los motivos que llevan a los jóvenes a estar en vulnerabilidad y violencia dentro de las

plataformas virtuales, creando ambientes incomodos y con riesgos hacia la integridad y privacidad de las personas, es por eso que se debe generar conciencia del buen uso de las redes sociales y generando estrategias para mitigar casos de ciberbullying y vulnerabilidad para que los estudiantes ya no sean un blanco fácil de las personas que buscan hacer daño. Este estudio se realizará mediante la recolección de información tipo encuesta, observación y charlas con los estudiantes buscando espacios de confianza para poder conocer el problema desde el fondo y poder hallar soluciones reales y concretas.

Teniendo en cuenta también que esto, generará el beneficio común, es un trabajo en equipo con estudiantes y docentes con un único fin que es velar por la seguridad de los jóvenes, implementando estrategias que faciliten los procesos educativos y de concientización, además conocer las plataformas que más se acomodan a las actividades pedagógicas y más seguridad brindan, encontrando los focos de inseguridad y vulnerabilidad que generan un mal ambiente dentro de las plataformas virtuales y así generar espacios más seguros y que se acomoden más a las necesidades de los planteles.

1.6 Marcos de Referencia

1.6.1 Marco Teórico – Conceptual

1.6.1.1 Amenazas riesgos y vulnerabilidades en redes sociales. Desde la llegada del internet a la sociedad la forma de interactuar y las relaciones interpersonales han cambiado notablemente, cada día se depende más de la virtualidad y esto se ha incrementado con la situación que se vive actualmente a nivel mundial, en donde todo se redujo en su gran mayoría a las pantallas y las interconexiones virtuales, aceptando que la vida cambio y que se debe aprovechar esa capacidad de adaptación que tienen los seres humanos y las evoluciones que se han presentado a lo largo de la historia. En su artículo, Peyró dice: "*Como mecanismo de adaptación y supervivencia formamos parte de diferentes grupos, desde la familia a los amigos, en todos los ámbitos, académicos, profesionales, culturales, etc. De este modo, los seres humanos estamos inmersos de manera permanente en una red de relaciones, y establecemos conexiones con nuestros iguales pues como seres sociales necesitamos relacionarnos, tomar contacto con el otro. Formamos parte de redes, y en ellas definimos y son definidos nuestros roles, nuestras relaciones, y en base a estas, obtenemos*

y transmitimos información relevante para diversos ámbitos de nuestra vida." (p. 236) como se lo menciona en la cita los seres humanos son seres que viven del cambio como Darwin lo dice en su Teoría de la evolución, el humano es un ser sometido al cambio en una guerra en la cual solo el más fuerte sobrevive, debido a esta teoría y esa mentalidad darwinista que caracteriza a los seres humanos la virtualidad se ha convertido en un reto, el cual como en toda especie viva unos se consideran más fuertes que otros. Peyró (2015, p 127)

Actualmente la seguridad informática es un término que compete a todas las ramas de la sociedad ya que, al vivir en un mundo globalizado, en donde se puede tener información de lo que pasa en todo el mundo, el educar para tener una seguridad en medio informáticos es un aspecto que viene desde casa y más en estos momentos en donde la llegada de nuevos equipos, redes y metodologías de enseñanza obligan a todas las personas mayores a educarse en temas de virtualidad para educar a los jóvenes. Según Aguilera: "se puede definir a la seguridad informática como la disciplina encargada de plantear y diseñar las normas, procedimientos, métodos y técnicas con el fin de obtener que un sistema de información sea seguro, confiable y sobre todo que tenga disponibilidad." (Aguilera, 2011 p 14) Para el periódico El Tiempo (2015) "Los papás de Colombia se están rajando en materia de cibercuidados con sus hijos. O por lo menos así lo sugieren las estadísticas sobre el crimen digital contra menores. El coronel Freddy Bautista director del Centro Cibernético de la Policía Nacional afirma que "Están disparados los robos de identidad digital, las amenazas, injurias y el 'grooming', en donde acosadores se hacen pasar por un niño o niña para engañar a menores de edad, a quienes luego invitan a intercambiar fotografías eróticas con las que después los extorsionan" lo cual lleva a entender que en Colombia el ciberespacio esta desprotegido y la vulnerabilidad en jóvenes ante las plataformas informáticas es grande. Periódico el tiempo (2015) ciberdelitos en jóvenes. La seguridad informática y la ciberseguridad buscan siempre proteger al usuario y su tarea es minimizar los riesgos que se corren en la realización de actividades de tipo informático, citando el texto Introducción a la seguridad informática y el análisis de vulnerabilidades: "Lo que debe contemplar la seguridad se puede clasificar en tres partes como son los siguientes: los usuarios, la información y la infraestructura. Los usuarios son considerados como el eslabón más débil de la cadena, ya que a las personas es imposible de controlar, un usuario puede un día cometer un error y olvidar algo o tener un accidente y este suceso puede echar a perder el trabajo de mucho tiempo, en muchos casos el sistema y la información deben de protegerse del mismo usuario. La información se considera como el oro de la seguridad informática ya que es lo

que se desea proteger y lo que tiene que estar a salvo, en otras palabras, se le dice que es el principal activo. Por último, está la infraestructura esté puede ser uno de los medios más controlados, pero eso no implica que sea el que corre menos riesgos, siempre dependerá de los procesos que se manejan. Se deben de considerar problemas complejos, como los de un acceso no permitido, robo de identidad, hasta los daños más comunes, por ejemplo, robo del equipo, inundaciones, incendios o cualquier otro desastre natural que puede tener el material físico del sistema de la organización." (Romero, Figueroa, Vera. 2018 p 28) como se puede observar en este apartado la seguridad informática es una cadena que tiene una interrelación con diferentes factores ya que para brindar una seguridad eficaz se debe minimizar riesgos en plataformas virtuales y generar conciencia del tratamiento de la información, no solo para las personas encargadas de recolectar dicha información sino para el usuario, generando así espacios cibernéticamente más seguros.

Las plataformas virtuales para la educación son actualmente los medios más usados para impartir los conocimientos académicos y desarrollar una vida escolar normal, la inclusión de las TIC en este medio ha hecho del aula escolar un aula 100% virtual, buscando ofrecer calidad en educación. Desde el año 2003 se habla de recursos educativos abiertos (REA) estos recursos son materiales didácticos de aprendizaje y educación que se pueden encontrar en las plataformas virtuales generando que la educación de calidad sea libre y dirigida a cualquier población, en cualquier parte del mundo. Ya que según la UNESCO esto aporta en la equidad social, la paz y la reconciliación, aquí podemos encontrar plataformas universales como: YouTube, Picasa, Scielo, Prezi, CmapTools, Wikipedia, entre otras.

En cuanto a la investigación se va hablar de lo que se convoca, la violencia, el ciberbullying y la vulnerabilidad de los jóvenes ante las plataformas virtuales, las generaciones actuales son generaciones que han nacido en un mundo globalizado, un mundo en el que la cultura cibernética domina, cultura que se basa en el desarrollo de la personalidad a través de las nuevas tecnología e información. es decir la vida se está centrando en las redes sociales y una vida desde las plataformas virtuales, es por esto que la vulnerabilidad de los jóvenes incrementa cada día, ya que hacen su información personal pública, arriesgan su seguridad y se hacen daño entre sí, la popularidad hace que se opaquen entre sí y la poca solidaridad genera afectaciones emocionales y psicológicas es por esto que todo aporte que se le haga el tema es de gran impacto y sobre todo la pedagogía que se pueda implementar.

1.6.1.2 Delitos informáticos y ciberseguridad. Debido al gran auge de la informática, la globalización, el uso indiscriminado de las redes sociales se han generado comportamientos inadecuados e ilícitos dentro de estas, a los cuales de los denomina "delitos informáticos" en Colombia se encuentran reglamentados por la ley 1273 de 2009 por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Básicamente esta ley busca penalizar a todas aquellas personas que hagan uso abusivo de las redes informáticas, suplantación de identidad, extorciones y violaciones a privacidad, modificación de datos que tienen un domino privado, etc.

En cuestión de ciberseguridad Colombia desde el año 2016 ha prendido fortalecer sus leyes y cuidado en el ámbito de la cibernética e informática, implementando un ColCERT que es un equipo que se encuentra a nivel nacional y se especializa en dar respuesta inmediata a problemas de seguridad informática, también el Banco Interamericano de Desarrollo, le aprueba un préstamo al país para desarrollar un programa denominado "Programa para la mejora de la conectividad y digitalización de la economía" con el cual se busca mejor las condiciones de ciberseguridad a nivel nacional, y posteriormente todos los años en MinTic ha buscado establecer convenios y generar a portes que mantengan a los colombianos seguros en cuestión de seguridad informática. Según el reporte de amenazas de Cisco (2019) los incidentes de seguridad más frecuentes son Botones y RAT (58%) y cryptoming (30%) otras amenazas como troyanos y suplantación de identidad se ven reflejados, pero con porcentajes inferiores al 10% esto quiere decir que los principales problemas de seguridad en el ambiente informático se dan por el robo y suplantación de criptomonedas o moneda de la virtualidad. Colombia está buscando renovarse y hacer el espacio cibernético más seguro por esta razón ha generado alianzas con entidades como la Interpol y Europol buscando reducir la delincuencia informática en el país a través agotando medio nacionales e internacionales.

1.6.1.3 Redes sociales e internet. El desarrollo y auge de las redes sociales ha ido de la mano con el desarrollo de la comunicación a través de ordenadores conectados por medio de una red que es el internet. El internet nace como un programa del cuerpo militar de estados unidos, convirtiéndose al momento como uno de los mayores inventos del hombre y generando una arquitectura informática libre con un acceso ilimitado y un avance cada vez mejor que permite

información globalizada, actualizada sobre diversos temas, en este contexto surgen las redes como medios informáticos que el mundo globalizado ha puesto a disposición de los seres humanos para compartir información ilimitada en cualquier parte del mundo en cuestión de segundos. Surgieron en 1995, con el fin mantener contacto entre estudiantes de los colegios o universidades de Estados Unidos, se crea un sitio web llamado ***"classmates.com."*** para los fines ya mencionados, poco a poco esto tomo mayor fuerza y en años posteriores aparecen redes sociales como Hi5, My Space, Hotmail, Facebook, entre otros. Actualmente las redes sociales mueven el mundo, son sitios web que permiten la interacción social, generan ingresos, promueven movimientos sociales y culturales y se han vuelto una parte fundamental en la vida de las personas, mediante esos medios se socializa, se mantienen relaciones interpersonales y se comunican casi de manera instantánea.

1.6.1.4 Educación desde la virtualidad. La educación virtual ha sido definida como la educación a distancia a través del ciberespacio, posible mediante la conexión y uso de internet, que no necesita de un tiempo y espacio específicos, que permite establecer un nuevo escenario de comunicación entre docentes y estudiantes (Bonilla, 2016). Según la ONU (UN, 2020a), los cierres de los espacios educativos y de aprendizaje han afectado al 94% de la población estudiantil mundial. Problema más acentuado aún en los países con escasos recursos. Las brechas de acceso se han incrementado con motivo de la pandemia, al reducir posibilidades a masas de estudiantes de poblaciones vulnerables o ya vulneradas. Esta crisis puede llevar a las poblaciones más pobres a una pérdida de aprendizaje irrecuperable, empujar al abandono de muchos estudiantes o a la dificultad para reiniciar las tareas escolares futuras debido, muy previsiblemente, a dificultades económicas generadas por la crisis. En concreto, las proyecciones de la ONU apuntan a que casi 24 millones de estudiantes de todos los niveles educativos podrían abandonar los estudios debido a dificultades económicas producidas por la pandemia (RIED, 2020)

Desde el año 2020 con la llegada de la pandemia COVID-19 se ha buscado establecer los lazos de la educación, la seguridad y la virtualidad. La educación virtual global llego en un ambiente de inmadurez y de falta de capacitación, pero, aun así, se desarrolló con el mayor esfuerzo posible para que profesores y estudiantes puedan desempeñar sus labores con eficacia y eficiencia. Esta etapa ha marcado un antes y un después, la virtualidad ha tomado una importancia sin precedentes y se ha convertido en una forma de educación donde se busca cumplir con los estándares adecuados desde la independencia del estudiante. En este panorama de educación virtual Colombia siendo un país

con un índice de pobreza de elevado según DANE 40% es decir que aproximadamente la mitad de los pobladores Colombianos tienen una vida por debajo de las condiciones aceptables, en este contexto la virtualidad se ha convertido en un problema económico y social, económico porque la deserción educativa en tiempos de pandemia aumento, la inasistencia de los estudiantes paso de un 2.7% a un 16.4% (DANE) especialmente en las veredas y zonas aleadas de Colombia, la falta de conectividad, la ausencia de medios informáticos y los riesgos de la cibernética generan preocupación en los padres pero los esfuerzos de la población siguen siendo altos para poder estudiar en medio de la emergencia sanitaria.

1.6.1.5 Contexto de la investigación, San Juan de Pasto. La investigación se la va a realizar en el municipio de San Juan de Pasto, ubicado en el suroccidente colombiano, según censo DANE cuenta con 460.638 habitantes, caracterizado por su riqueza cultural, nace en las faldas de un volcán que es sinónimo de fuerza para la región. A lo largo de la historia Pasto ha sido un municipio marcado por la tradición y aspecto religioso denominándose así “la ciudad Teológica” (POT, 2012 p 12)

1.6.1.6 Contexto de la Institución Educativa Municipal Ciudad de Pasto. La institución en la que se realizará el proyecto es la Institución Educativa Municipal Ciudad Pasto, colegio que cuenta actualmente con tres sedes en el municipio, colegio fundado en 1957 por el señor José Senén Braveen aquel tiempo se desempeñaba como Fiscal del Sindicato de Carpinteros de Pasto; apoyado por esa organización, emprende la gestión en procura de la creación de un colegio que llevara el nombre de la muy noble Ciudad de Pasto. Para ese entonces, el contexto educativo en la capital de Nariño, se caracterizaba por el alto costo de las matrículas, pensiones y textos; la falta de centros educativos, injustificados requisitos para el ingreso a la educación, la escasez de trabajo, carestía de alimentos, aumento exagerado de precios y la indiferencia absoluta de las autoridades. Fue así como mediante ordenanza N.º 51 de noviembre 30 de 1.958, emanada de la Honorable Asamblea Departamental de Nariño, la misma que fuera sancionada por el entonces Gobernador, Dr. Jorge Rasero Pastrana, se crea el Colegio Ciudad de Pasto, para atender la educación secundaria a estudiantes de ambos sexos. Actualmente el colegio es reconocido por su calidad educativa por tener espacios de inclusión educativa como deportes para personas con capacidades diferentes, además cuenta con banda de paz, escuela de danza y ballet folclórico, escuela de música, entre otros aspectos que complementan la actividad académica de los niños y jóvenes de la ciudad de pasto. En esta

institución se busca hacer un análisis de la vulnerabilidad en redes sociales de los jóvenes estudiantes de municipio de Pasto.

1.7 Metodología

1.7.1 Paradigma, enfoque y tipo de investigación

El paradigma de investigación del presente trabajo es cuantitativo con un enfoque empírico analítico, el cual, se basa en conocer una realidad desde los ojos de la objetividad, en donde los prejuicios, valores y moralidades no tienen campo y los datos se analizan con métodos netamente numéricos y estadísticos buscando las interpretaciones más racionales que se le puede dar al problema en cuestión. Según Roberto Sampieri Hernández, experto en metodologías de la investigación: "El enfoque cuantitativo utiliza la recolección y el análisis de datos para contestar preguntas de investigación y probar hipótesis establecidas previamente, y confía en la medición numérica, el conteo y frecuentemente en el uso de la estadística para establecer con exactitud patrones de comportamiento en una población." Sampieri (2014, p 33)

La investigación es de tipo exploratoria, debido a la poca información que hay sobre el tema de vulnerabilidad en las plataformas virtuales en estudiantes, cabe resaltar que la vulnerabilidad cibernética ha sido trabajada en otras investigaciones, pero en contextos diferentes al educativo, la información sobre el área de vulnerabilidad de las plataformas virtuales en el área de la educación ha sido poco trabajada tanto en el territorio nacional como departamental y municipal. Citando a Fernández, Hernández y Baptista quienes en su libro Metodología de la Investigación afirman que

"La investigación exploratoria, se efectúa normalmente cuando el objetivo a examinar un tema o problema de investigación poco estudiado, del cual se tienen muchas dudas o no se ha abordado antes" Fernández & Baptista & Hernández (2012, p 39)

Con los aportes dados y el sustento teórico se concluye que esta investigación es de corte cuantitativo, buscando recolectar la información necesaria que permita conocer el problema de la vulnerabilidad en jóvenes estudiantes a fondo y analizarlo de manera muy objetiva, clara y precisa.

1.7.2 Línea y Áreas Temáticas de investigación

Línea de investigación: Ingeniería, Informática y computación.

Áreas Temáticas de investigación: Informática educativa, pedagogía y currículo

1.7.3 Población y muestra

La población para el estudio son los estudiantes de grado decimo y once de la I.E.M. Ciudad de Pasto los cuales según listados oficiales son 840 estudiantes en las dos jornadas.

Se trabajará con un muestreo intencional, en donde el investigador selecciona la muestra según criterio propio, se decide escoger al azar a 10 estudiantes por cada salón, teniendo como resultado una muestra de 240 estudiantes. El muestreo intencional según el autor McMillan & Schumacher en su libro "Investigación educativa" es: "*un muestreo en el que el investigador selecciona elementos particulares a partir de una población que será representativa o proporcionará información sobre el elemento de interés. Sobre la base del conocimiento que tiene el investigador de la población, se hace un juicio sobre qué sujetos deberían ser seleccionados para proporcionar la información más adecuada que responda al propósito de la investigación*"

1.7.4 Proceso de investigación

Tabla 1

Proceso de investigación

Objetivos específicos	Fuente	Técnica de recolección	Instrumento	Técnica de Procesamiento	Resultado
Identificar la información y los recursos informáticos que maneja la IEM Ciudad de Pasto en sus procesos educativos.	Observación , visitas a la institución, entrevistas con los encargados de cada área.	Diario de campo	Diario de campo, documento con la descripción de la institución y tabla de recursos e información.	Análisis descriptivo.	Informe de los recursos informáticos que posee la institución y descripción de cada área.
Determinar vulnerabilidades, riesgos y amenazas en medios informáticos usados para la virtualidad en el proceso pedagógico en grados decimo y once de la institución objeto de estudio, bajo metodología Magerit e ISO/IEC 27000	Bases de datos de estudiantes de grado 10 y 11 de la I.E.M. Ciudad de Pasto. Informes de internet, sitios web, blogs, libros e informes de denuncias de delitos informáticos en colegios.	Encuestas a estudiantes de los grados 10 y 11 del colegio objeto de estudio.	Formulario en Google Forms.	Estadística inferencial, y análisis cualitativo de cruces variables.	Informe sobre las vulnerabilidades en medios informáticos usados para la virtualidad en el proceso pedagógico de los estudiantes.
Diseñar una propuesta para el mejoramiento de	Documentos de resultados	Revisión documenta l y de resultados.	Base de datos que arroja la encuesta,	Análisis de datos y resultados.	Socialización del informe de análisis de

Objetivos específicos	Fuente	Técnica de recolección	Instrumento	Técnica de Procesamiento	Resultado
la seguridad informática en la institución educativa objeto de estudio.	del proceso de investigación		bibliografía sobre los problemas encontrados , fichas de revisión documental y análisis de resultados.		riesgos y vulnerabilidades que corren los estudiantes dentro de los procesos pedagógicos y como se puede mejorar la seguridad en estos espacios.

1.7.5 Variables e hipótesis

Hipótesis:

Se han presentado diversas vulnerabilidades en el uso de las redes sociales y sistemas informáticos en procesos pedagógicos mediados por tecnología en la I.E.M. Ciudad de Pasto en el año 2023.

Variables:

Tabla 2

Variables

Variable	Descripción	Tipo de Variable	Objetivo especifico	Indicador	Naturaleza	Fuente	Tr*	Ta**
Vulnerabilidad	Esta variable es dependiente de orden cualitativo, la cual permite identificar el	Dependiente	Identificar las caracterísitcas de las vulnerabilidades que se presentan en sistemas	Ataques cibernéticos que se hayan sufrido en el último año.	Cualitativa	Estudiantes de grado 10 y 11 de la I.E.M. Ciudad de Pasto del año 2023	Encuestas	Análisis multivariados.

Variable	Descripción	Tipo de Variable	Objetivo especifico	Indicador	Naturaleza	Fuente	Tr*	Ta**
	grado y tipo de vulnerabili-dad a los que los jóvenes están expuestos mediante los procesos escolare s en la I.E.M. Ciudad de Pasto		informáticos mediante el uso de redes sociales o sistemas informáticos.	Porcentaje de vulnerabilidad en la que se ubica el estudiante ante el uso de redes sociales y plataformas virtuales Porcentaje de seguridad que le da a sus redes y plataformas virtuales				
Riesgo	Esta variable es independiente de orden cualitativo la cual mide el riesgo que los jóvenes corren con el uso de los sistemas de información virtual y redes sociales que se usan en el proceso pedagógico en la I.E.M. Ciudad de Pasto	Independiente	Identificar situaciones de riesgos y vulnerabilidades más recurrentes presentadas por el uso de redes sociales y plataformas educativas en procesos pedagógicos en instituciones educativas en el país.	Factores de riesgo más recurrentes en el último año. Riesgo en redes sociales. Riesgos en las plataformas de educación virtual ciberbullying	Cualitativa	Estudiantes de grado 10 y 11 de la I.E.M. Ciudad de Pasto	Encuestas	Análisis multivariados.

* Técnica de recolección

**Técnica de análisis (Ubicar en página horizontal)

1.8 Presupuesto

Tabla 3

Presupuesto global del proyecto

Rubros	Total ($)
Inversión en personal	969.088
Otros rubros	2.080.000
Total	**3.049.088**

Tabla 4

Descripción de la Inversión en personal.

Nombre Investigador	Vr. Hora Investigador	Dedicación Número total de horas	Valor
Javier Villalba	$15.142	32	$484.544
David Sebastián Martínez	$7.571	64	$ 484.544
Camilo Andrés Bravo Rosero	$7.571	64	$ 484.544
TOTAL			**$ 1.453.632**

Tabla 5

Presupuesto de materiales y equipos.

Rubro	Justificación	Valor total
Equipos	Alquiler y depreciación de equipos	1280000

	de computo	
Materiales	CD, USB, Tinta de impresora, resma de papel, empastes.	200000
Software	No aplica	0
Bibliográfica	No aplica	0
Eventos académicos	Seminario	300000
Publicaciones	Publicación revista indexada	200000
Salidas de campo	Transporte	100000
Viajes		0
	TOTAL	2.080.000

1.9 Cronograma

Tabla 6

Cronograma

Actividades	Tiempo											
	1	2	3	4	5	6	7	8	9	10	11	12
Identificar la información y los recursos informáticos que maneja la IEM Ciudad de Pasto en sus procesos educativos.												
• Visita a la institución es objeto de estudio.	X	X	X	X	X							
• Observación de recursos y encuesta con las personas encargadas de cada área.						X	X	X	X			
• Elaboración de documento donde se describa los recursos que posee la institución y otros factores relevantes para la investigación.										X	X	X
Determinar las vulnerabilidades en medios informáticos usados para la virtualidad en el proceso pedagógico en grados decimo once de las instituciones objeto de estudio.												
• Aplicación de encuestas a los estudiantes objetivo de investigación	X	X	X	X								
• Análisis de base de datos				X	X	X						
• Revisión bibliográfica sobre los hallazgos							X	X				
• Elaboración de documento sobre el análisis de resultados.									X	X	X	X
Diseñar una propuesta para el mejoramiento de la seguridad informática en la institución educativa objeto de estudio.												
• Análisis de resultados	X	X	X	X								
• Revisión de informes					X	X	X	X				
• Socialización de los resultados y las recomendaciones para la institución									X	X	X	X

1.10 Productos Esperados

Monografía: Documento con los resultados de la investigación y acorde con los lineamientos institucionales.

Artículo científico: Articulo con la síntesis de los resultados que será publicado en revista de la Universidad Mariana o en otra de circulación académica.

Ponencia en evento académico: Los resultados de la investigación se divulgarán en una ponencia de un evento de orden local o nacional.

2. Desarrollo del Proceso Investigativo

2.1 Información y Recursos Informáticos de la IEM Ciudad de Pasto

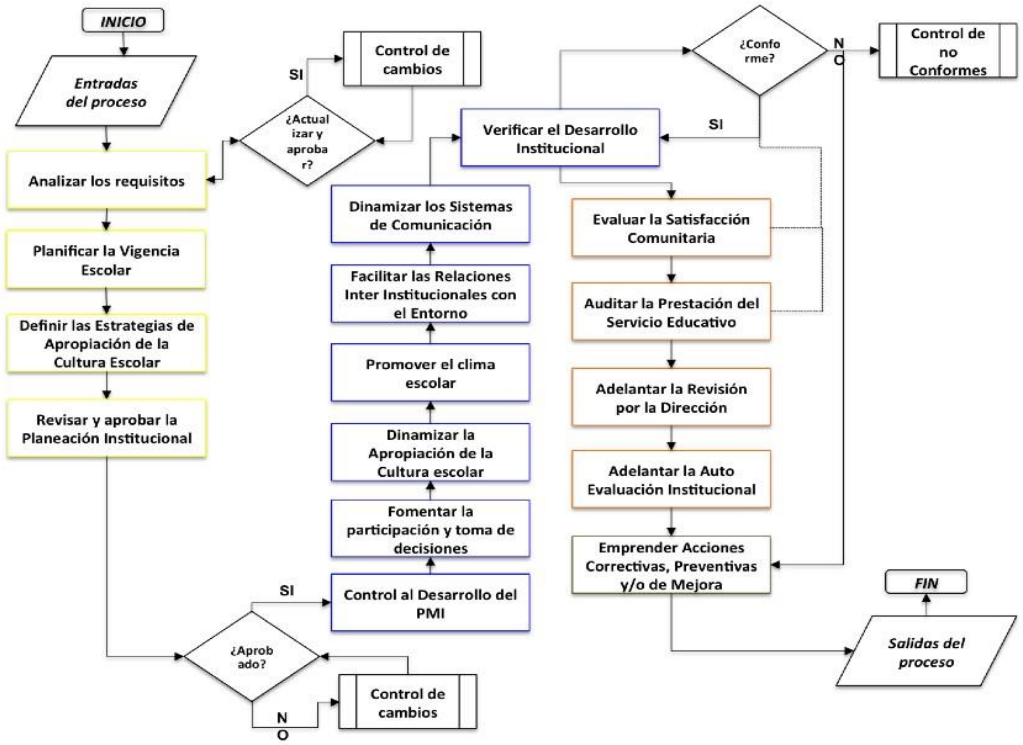
La IEM Ciudad de Pasto es una institución consolidada hace 65 años, está divida en 4 áreas de gestión estas son:

Gestión directiva: Está integrada por el señor Rector José Vicente Guancha, 9 coordinares de convivencia y académicos, 2 docentes orientadoras y 2 docentes gestoras de la inclusión dentro de la institución, esta área es la encargada de la programación académica para la acción orientada a ayudar a mejorar los procesos formativos y disciplinarios aplicando las normas establecidas por el ministerio de educación con propuestas de abrir nuevos proyectos y velar con el excelente funcionamiento del plantel educativo.

El proceso inicia con la entrada de requisitos que deben ser analizados meticulosamente. Luego, se procede a planificar la vigencia escolar, definiendo estrategias para la apropiación de la cultura escolar. Una vez establecida la planificación institucional, se lleva a cabo su revisión y aprobación. Si es aprobada, se continúa con el control de cambios y la verificación del desarrollo institucional. Se dinamizan los sistemas de comunicación y se facilitan las relaciones interinstitucionales con el entorno. Se promueve un clima escolar positivo y se fomenta la participación y toma de decisiones. Se evalúa la satisfacción comunitaria y se audita la prestación del servicio educativo. Además, se realizan acciones correctivas, preventivas y/o de mejora, si es necesario. Finalmente, se llevan a cabo la revisión por la dirección y la autoevaluación institucional antes de concluir el proceso con las salidas correspondientes. Esta área se encarga de analizar y definir las estrategias académicas como se muestra en la Figura 1.

Figura 1

Diagrama de flujo de gestión Directiva.



Fuente: IEM, Ciudad de Pasto (2023), sitio web áreas de gestión. Diagrama de flujo de datos del proceso de gestión Directiva. Recuperado de https://www.iemciudaddepasto.edu.co/gestiondirectiva/.

Gestión académica: Está integrada por toda la planta de docentes de la institución tanto de bachillerato como primaria y las diferentes sedes. El área de gestión académica se divide en 12 subáreas que son:

- Ciencias Naturales: Comprender el mundo natural y asumir sus compromisos ecológicos, por medio de la aproximación científica al conocimiento.
- Matemáticas: Pensar matemáticamente para comunicar, razonar, plantear y resolver problemas de la vida cotidiana, la ciencia y la tecnología.
- Filosofía: Reflexionar sobre el sentido de la existencia, los problemas del mundo social y la relación entre lo ético y estético en la vida de los seres humanos.

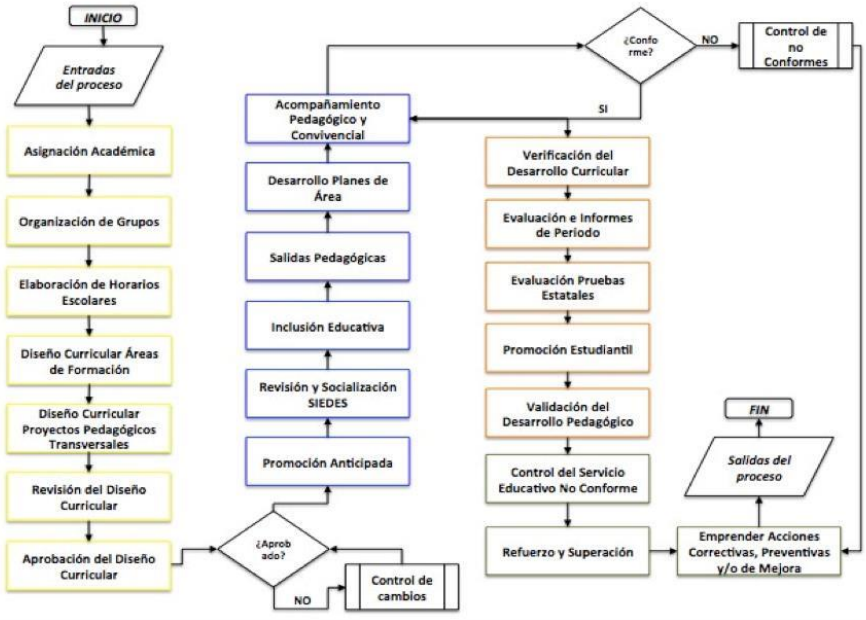
- Lenguaje: Establecer comunicaciones efectivas y significativas que fortalezcan la reciprocidad e interacción con sus congéneres y las culturas.
- Ciencias sociales: Comprender el mundo social y asumir sus responsabilidades ciudadanas, por medio de la aproximación científica al conocimiento.
- Inglés: Utilizar sus habilidades comunicativas en lengua extranjera (inglés) para interactuar y comprender otras culturas.
- Educación artística: Apreciar y comprender el valor artístico de las manifestaciones culturales y promover la expresión estético-_ comunicativa.
- Educación física: Fortalecer su calidad de vida por medio de la práctica de actividades
- Físicas, lúdicas y deportivas ○ Tecnología: Utilizar asertivamente las herramientas tecnológicas, informáticas y comunicativas para procesar información y resolver problemas.
- Educación religiosa: Vivir su experiencia de fe y descubrir su dimensión trascedente desde el plano espiritual, social y ambiental.
- Ética y valores: Asumir una posición ética que contribuya al bienestar y el desarrollo sostenible de la persona, la sociedad y el ambiente.
- Preescolar: facilitar la adaptación a la vida escolar, afianzar conocimientos sobre los valores, destrezas y capacidades fundamentales del desarrollo del ser humano.

Las fases de la gestión académica como se muestra en la figura 2, al mismo tiempo abarca la asignación, elaboración diseño y aprobación del desarrollo curricular acorde al SIEDES (Sistema institucional de Evaluación de estudiantes) El proceso se inicia con la asignación académica y la organización de grupos, seguidos de la elaboración de horarios escolares. Se procede con el diseño curricular de las áreas de formación y de los proyectos pedagógicos transversales, los cuales son revisados y posteriormente aprobados. Se brinda acompañamiento pedagógico y convivencial, además de desarrollar planes para salidas pedagógicas. Se aborda el área de inclusión educativa y se realiza la revisión y socialización correspondiente. Si el proceso es aprobado, se promueve la promoción anticipada; de lo contrario, se lleva a cabo el control de cambios. Se verifica el desarrollo curricular y se elaboran evaluaciones e informes periódicos, incluyendo pruebas estatales. Finalmente, se procede con la promoción estudiantil y la validación del desarrollo

pedagógico, tomando medidas correctivas, preventivas o de mejora en caso de necesidad antes de concluir el proceso con las salidas correspondientes.

Figura 2

Diagrama de flujo de gestión académica



Fuente: IEM, Ciudad de Pasto (2023), sitio web áreas de gestión. Diagrama de flujo de datos del proceso de gestión académica Recuperado de https://www.iemciudaddepasto.edu.co/gestion-academica/.

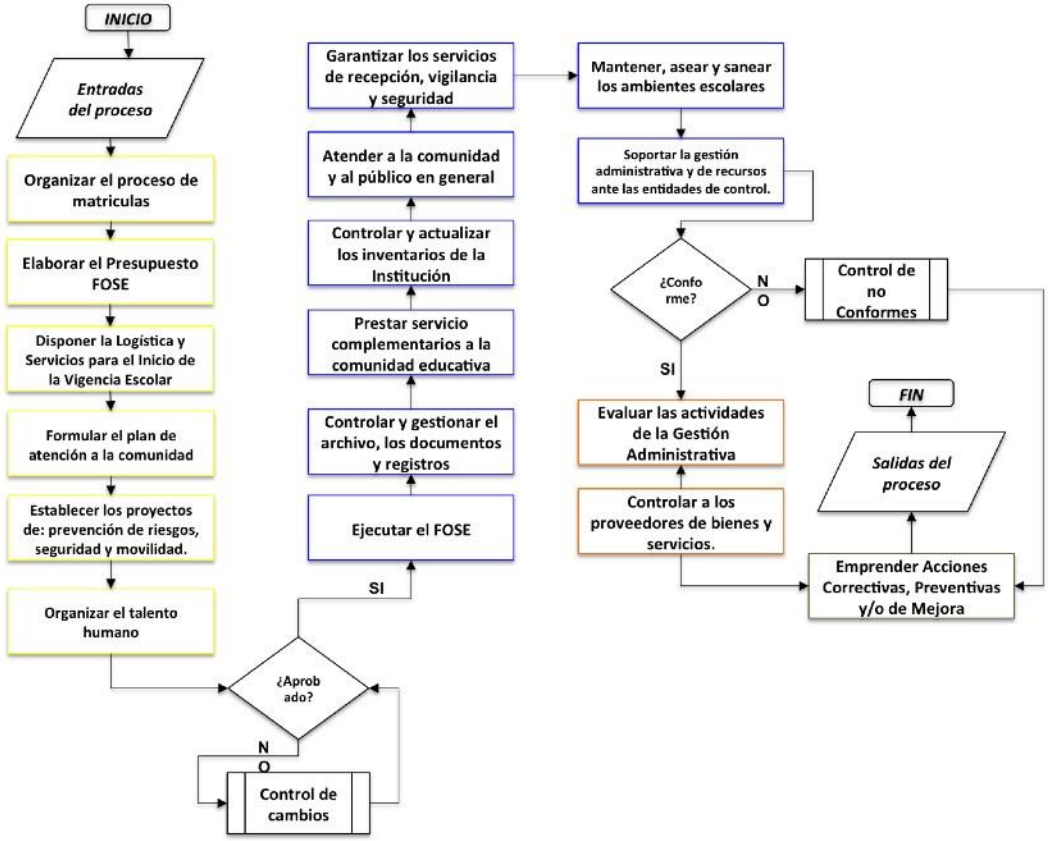
Gestión administrativa y financiera: Es la encargada del manejo del talento humano, recursos para prestar un servicio eficiente y en las mejores condiciones, en esta área están las subáreas de: tesorería, biblioteca, ambientes educativos y servicios generales, estas áreas tienen relación directa con planeación, desarrollo, evaluación y mejoramiento de la institución a través de un proceso de intervención continuo y oportuno.

Como se puede observar en la figura 3. El proceso de organización de matrículas comienza con una serie de actividades, desde la elaboración del presupuesto hasta la disposición de la logística y los servicios necesarios para el inicio del año escolar. Se formula un plan de atención a la comunidad y se establecen proyectos de prevención de riesgos, seguridad y movilidad. Se organiza el talento humano y se garantizan los servicios esenciales de recepción controlados siguiendo el

orden con las ejecuciones del FOSE (Fondos de Servicios Educativos), vigilancia y seguridad, así como la atención a la comunidad en general. Se lleva a cabo el control y actualización de inventarios, la gestión de archivos y documentos, y se presta servicios complementarios a la comunidad educativa. Una vez ejecutado el plan, se evalúan las actividades administrativas y se controlan los proveedores de bienes y servicios. En caso de discrepancias o no conformidades, se emprenden acciones correctivas, preventivas o de mejora para asegurar la eficacia del proceso.

Figura 3

Diagrama de flujo de gestión administrativa y financiera.



Fuente: IEM, Ciudad de Pasto (2023), sitio web áreas de gestión. Diagrama de flujo de datos del proceso de gestión Administrativa y financiera. Recuperado de https://www.iemciudaddepasto.edu.co/gestion-administrativa-y-financiera/.

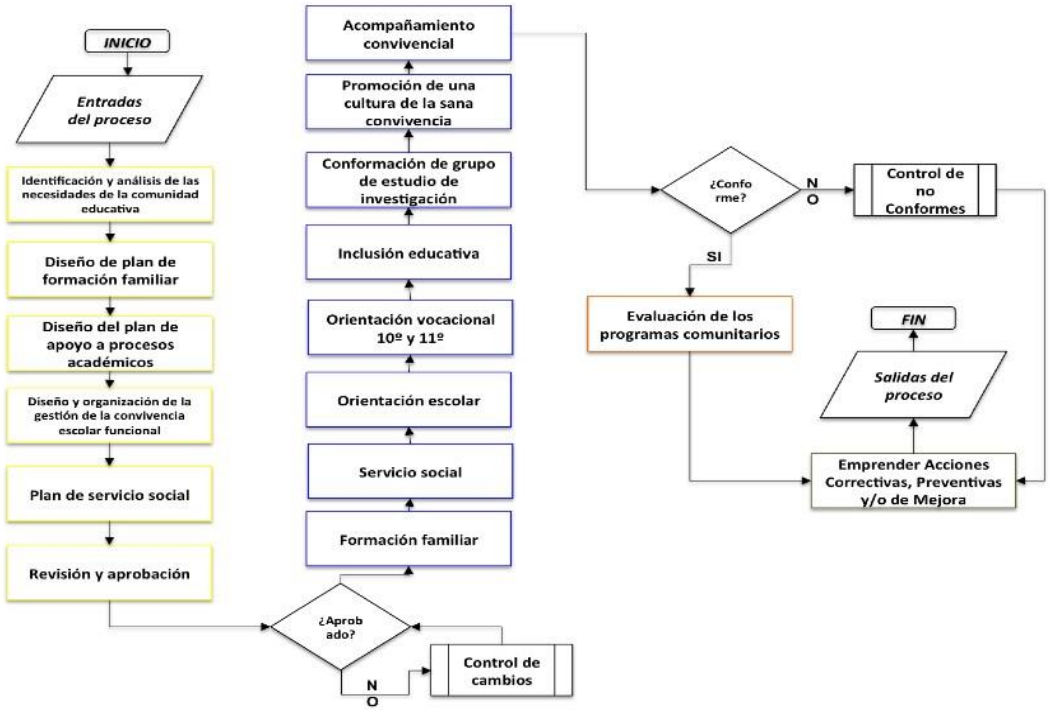
Gestión comunitaria: Busca contribuir con el bienestar comunitario y mantener un buen ambiente escolar, esta área se encarga del acompañamiento psicológico, social y nutricional de los

integrantes de la comunidad educativa, en esta área se incluye orientación escolar, la enfermería institucional y el comedor estudiantil.

El proceso comienza con la identificación y análisis de las necesidades de la comunidad educativa, seguido del diseño de planes de formación familiar, apoyo a procesos académicos y gestión de la convivencia escolar. Se establece un plan de servicio social y se promueve una cultura de sana convivencia. Además, se conforma un grupo de estudio de investigación y se brinda orientación vocacional y escolar, especialmente para los grados 10° y 11°. Tras la revisión y aprobación, se acompaña convivencialmente a la comunidad educativa, y se evalúan los programas comunitarios implementados. Si se detectan no conformidades, se realizan acciones correctivas, preventivas o de mejora para garantizar la efectividad del proceso**.** Tal como se observa en la figura 4.

Figura 4

Diagrama de flujo de la gestión comunitaria



Fuente: IEM, Ciudad de Pasto (2023), sitio web áreas de gestión. Diagrama de flujo de datos del proceso de gestión comunitaria Recuperado de https://www.iemciudaddepasto.edu.co/gestion-comunitaria/.

Una vez identificadas las áreas de la institución y sus funciones se proceden a identificar y listar los activos informáticos de la institución, usando para ello el estándar ISO/TEC 27001 con el fin de determinar con exactitud cada uno de los activos informáticos y en un siguiente apartado determinar riesgos y vulnerabilidades. Al momento de la observación se encuentra en la institución los siguientes activos

2.2 Identificación de Activos

Para comenzar, se lleva a cabo la identificación, clasificación y catalogación de todos los activos de información que se encuentran en la infraestructura de la Institución Educativa Municipal San Juan de Pasto y que son parte del ámbito del Sistema de Gestión de Seguridad de la Información (SGSI), es decir, del proceso de gestión de la información.

En el proceso de identificación se establece el nombre del activo, el responsable del proceso o propietario del activo, y la categoría a la que pertenece dicho activo.

El activo se clasifica como uno de los siguientes tipos:

- [D] Datos / Información
- [K] Claves Criptográficas
- [S] Servicios
- [SW] *Software* / Aplicaciones informáticas
- [HW] Equipamiento informático (*hardware*)
- [COM] Redes de comunicaciones
- [Media] Soportes de información
- [AUX] Equipamiento auxiliar
- [P] Personal

Es fundamental llevar a cabo una catalogación precisa debido a que esta permite la identificación de amenazas que podrían aprovechar una o más vulnerabilidades. Posteriormente, se determina el nivel de riesgo de cada una y se elabora un plan de tratamiento correspondiente para mitigarlos.

Activos que posee la institución

- **Equipos informáticos:** Esto incluye computadoras de escritorio, computadoras portátiles, proyectores, pizarras interactivas y otros dispositivos utilizados para la enseñanza y el aprendizaje.
- **Datos y acceso credenciales:** Correos electrónicos como personales institucionales y accesos especiales entre otros.
- **Servidores:** Los servidores son utilizados para almacenar datos, aplicaciones y servicios en la red de la institución educativa. Pueden incluir servidores de archivos, servidores de aplicaciones, servidores de correo electrónico, servidores de bases de datos, entre otros
- **Software de gestión del aprendizaje (LMS):** La institución educativa tiene un software educativo instalado en sus equipos para el desarrollo de las clases.
- **Red de área local (LAN):** La infraestructura de red local conecta todos los dispositivos dentro de la institución educativa. Esto incluye cables de red, switches, routers, puntos de acceso inalámbrico.
- **Recursos en la nube:** La institución puede utilizar servicios en la nube para almacenar datos, ejecutar aplicaciones y respaldar sistemas. Esto puede incluir servicios de almacenamiento en la nube, plataformas de colaboración en línea, herramientas de gestión de documentos.
- **Sistemas de gestión de información escolar (SIS):** Estos sistemas son utilizados para gestionar la información académica y administrativa de la institución, incluyendo la inscripción de estudiantes, la planificación de cursos, la gestión de calificaciones.

  SAPRED. Sistema que se encarga en todo el registro de notas que usa referente a la academia.

  SIMAD: Sistema de matrículas.

  SECOD: Sistema de contratación; rectoría, para abrir recursos, convocatoritas.

  CAFI: plataforma de prevención que se encarga y busca dar capacitaciones a estudiantes y a padres de familia, en áreas especiales.

  Sistema maestro: Es un sistema especializado del ministerio

  SEM: Sistema para el registro que utiliza la Institución todo referente para la educación inclusiva, con discapacidad y para el registro.

- **Reputación institucional:** La representación visual y la impresión que los grupos tienen de la empresa, derivadas de sus acciones tanto dentro como fuera de la organización.

2.2.1 Inventario de activos informáticos del área administrativa de la IEM Ciudad de Pasto

El área administrativa de la IEM Ciudad de Pasto está compuesta por las siguientes oficinas: rectoría, secretaria académica y financiera, atención al ciudadano, contaduría y servicios generales. Es la encargada del manejo de personal, administración de recursos económicos, toma de decisiones importantes para el plantel, manejo de cuentas y otras actividades.

Tabla 7

Inventario de activos informáticos de la IEM Ciudad de Pasto (Área administrativa)

Tipo	Nombre del activo
[SW] Software - Aplicaciones informáticas	1. Paquetes office 2. Sapred 3. SIMAT 4. Compucontact
[S] Servicios	5. Conexión a internet (Wifi – Cable)
[COM] Redes de comunicación	6. Router proveedor de servicios de internet (1) 7. Telefonía fija
[HW] Equipamiento informático (hardware)	8. Impresora hp laserjet P2035 (2) 9. Impresora oki mp85501b (1) 10. Computadores de escritorio (5) 11. Computadores portátiles (3) 12. Televisores (3)
[AUX] Equipamiento auxiliar	13. Cableado de red UTP 14. Cableado de telefonía
[P] Personal	15. Rector 16. Funcionarios del área administrativa, financiera y manejo de personal

2.2.2 Inventarios de activos informáticos del área informática de la IEM Ciudad de Pasto

El área informática de la IEM Ciudad de Pasto está compuesta por los siguientes espacios académicos: oficina de redes informáticas y 4 aulas educativas. La oficina de redes es la encargada del manejo de software, comunicaciones, hardware, reparaciones de equipos, entre otras actividades relaciones con los equipos informáticos y 4 aulas de ayuda educativa la cual se usa para la impartición de conocimiento y manejo de la tecnología.

Tabla 8

Inventario de activos informáticos de la IEM Ciudad de Pasto (Área informática)

Tipo	Nombre del activo
[SW] Software - Aplicaciones informáticas	1. Paquetes office 2. Sapred 3. SIMAT
[S] Servicios	4. 4. Conexión a internet (Wifi – Cable)
[COM] Redes de comunicación	5. Router proveedor de servicios de internet (4) 6. Telefonía fija
[HW] Equipamiento informático (hardware)	7. Impresora HP P1006 (1) 8. Computadores de escritorio (31) 9. Computadores portátiles (133) 10. Televisores (5)
[AUX] Equipamiento auxiliar	11. Cableado de red UTP 12. Cableado de telefonía
[P] Personal	13. Ingeniero de sistemas 14. Docentes área de informática

Fuente: Autoría propia.

2.2.3 Inventario de activos informáticos del área académica de la IEM Ciudad de Pasto

El área académica de la IEM Ciudad de Pasto está compuesta por los siguientes espacios coordinación académica y 16 salones de estudios. El área académica es la encargada de establecer, orientar y desarrollar todos los procesos académicos de la institución y los salones de los grados objeto de estudio que cada uno de ellos cuenta con un elemento tecnológico para el desarrollo de las actividades académicas.

Tabla 9

Inventario de activos informáticos de la IEM Ciudad de Pasto (Área académica)

Tipo	Nombre del activo
[SW] Software - Aplicaciones informáticas	1. Paquetes office 2. Sapred 3. SIMAT
[S] Servicios	4. 4. Conexión a internet (Wifi – Cable)
[COM] Redes de comunicación	5. 5. Router proveedor de servicios de internet (2)
[HW] Equipamiento informático (hardware)	6. Impresora hp laserjet P1006 (1) 7. Computadores de escritorio (2) 8. Computadores portátiles (5) 9. Televisores (16) 10. Video bean (6)
[AUX] Equipamiento auxiliar	11. Cableado de red UTP 12. Cableado de telefonía
[P] Personal	13. Coordinador académico 14. Docentes de la institución

2.2.4 Inventario de activos informáticos del área de convivencia de la IEM Ciudad de Pasto

El área de convivencia de la IEM Ciudad de Pasto está compuesta por los siguientes espacios coordinación de convivencia, orientación escolar y apoyo escolar. El área de convivencia es la encargada de orientar todos los procesos psicológicos y de acompañamiento escolar de la institución, también el área de inclusión educativa.

Tabla 10

Inventario de activos informáticos de la IEM Ciudad de Pasto (Área convivencia)

TIPO	NOMBRE DEL ACTIVO
[SW] Software - Aplicaciones informáticas	1. Paquetes office 2. Sapred 3. SIMAT 4. COPES
[S] Servicios	5. Conexión a internet (Wifi – Cable)
[COM] Redes de comunicación	6. Router proveedor de servicios de internet (1) 7. Telefonía fija
[HW] Equipamiento informático (hardware)	8. Computadores de escritorio (2) 9. Computadores portátiles (2) 10. Televisores (1)
[AUX] Equipamiento auxiliar	11. Cableado de red UTP
[P] Personal	12. Coordinador de convivencia 13. Docentes orientadores

Fuente: Autoría propia

2.3 Descripción del Área de Rectoría de la IEM Ciudad de Pasto

La rectoría es la encargada de la planeación, desarrollo, evaluación, y mejoramiento continuo del Proyecto Educativo Institucional, el rector de la institución se encarga de la gestión académica y administrativa y la toma de decisiones importantes para el plantel educativo, en la tabla No. 11

se detalla los recursos informáticos que usa el área de rectoría, plataformas virtuales más usadas y medios de almacenamiento de información, complementando la información dada anteriormente en el inventario del área administrativa de la institución.

Tabla 11

Descripción área de rectoría IEM Ciudad de Pasto

Área	Tareas a desarrollar dentro de la institución	Recursos informáticos	Cantidad	Plataformas virtuales más usadas	Procesamiento de la información		Almacenamiento y administración de datos
					Manual	Autom.	
Rectoría (Directivo)	Encargada del funcionamiento y administración de la institución	Computador portátil Computador de escritorio Impresora Televisor de 45”	1 1 1 1	Paquete office SAPRED SIMAT SECOP Sistema Maestro	X		Discos duros internos de los equipos, archivo de documentos y nube.

Fuente: Autoría propia

2.3.1 Descripción del área de coordinación académica y de convivencia de la IEM Ciudad de Pasto

Las coordinaciones de la institución educativa son las encargadas de llevar a cabo actividades que mantengan el orden y la convivencia, preside los comités y planes de convivencia, orienta a los padres de familia cuando hay un problema dentro de la institución, programa los horarios de los docentes con las jornadas de vigilancia, establece unión con el área de orientación escolar y busca tener un acompañamiento eficaz a cada integrante de la institución educativa. En la tabla No. 11 se hace una descripción de las áreas de coordinación de la institución, detallando las tareas a desarrollar, recursos informáticos utilizados, plataformas virtuales y medios de almacenamiento de los datos, como se observa a continuación.

Tabla 12

Descripción área de coordinación académica y de convivencia IEM Ciudad de Pasto

Área	Tareas a desarrollar dentro de la institución	Recursos informáticos	Cantidad	Plataformas virtuales más usadas	Procesamiento de la información		Almacenamiento y administración de datos
					Manual	Autom.	
Coordinación Académica	Encargada de la planeación y ejecución de los planes de estudios y programación escolar de la institución.	Computador de escritorio Impresora	1 1	SAPRED SEM	X		Archivo de documentos físicos en las carpetas estudiantiles, discos duros internos.
Coordinación de convivencia	Encargada de vigilar los procesos diarios que se llevan a cabo en la institución, orientar a padres de familia y docentes, vigilar que las normas se cumplan dentro de la institución y haya un ambiente sano en el	Computador de escritorio Impresora	1 1	SEM CAFI	X		Archivo de documentos físicos en las carpetas estudiantiles, discos duros internos.

	plantel educativo						

Fuente: Autoría propia

2.3.2 Descripción de las aulas informáticas de la IEM Ciudad de Pasto

Las aulas de informática de la institución son las herramientas utilizadas por los docentes para la correcta utilización de los medios informáticos, tecnológicos y comunicativos, en las aulas se desarrollan actividades de tipo académico en las cuales los estudiantes adquieren el conocimiento básico en las TIC según su nivel educativo, como se observa en la taba No. 13 hay una descripción de cada aula informática.

Tabla 13

Descripción aulas de informática IEM Ciudad de Pasto

Área	**Tareas a desarrollar dentro de la institución**	**Recursos informáticos**	**Cantidad**	**Plataformas virtuales más usadas**	**Procesamiento de la información**		**Almacenamiento y administración de datos**
					Manual	**Autom.**	
Aula de informática # 1	Impartir clase de aquellas asignaturas que requieran el uso de algún software especializado o acceso a Internet	Computador de escritorio Equipo de cómputo portátil	1 40	SAPRED SEM	X		Archivo de documentos físicos en las carpetas estudiantiles, discos duros internos.
Aula de informática # 2	Impartir clase de aquellas asignaturas	Computador de escritorio Equipo de cómputo	1 40	SAPRED SEM	X		Archivo de documentos físicos en las carpetas

	que requieran el uso de algún software especializado o acceso a Internet	portátil				estudiantiles, discos duros internos.
Aula de informática # 3	Impartir clase de aquellas asignaturas que requieran el uso de algún software especializado o acceso a Internet	Computador de escritorio Equipo de cómputo portátil	28 13	SAPRED SEM	X	Archivo de documentos físicos en las carpetas estudiantiles, discos duros internos.
Aula de informática Galileo	Impartir clase de aquellas asignaturas que requieran el uso de algún software especializado o acceso a Internet	Computador de escritorio Equipo de cómputo portátil	1 40	SAPRED SEM	X	Archivo de documentos físicos en las carpetas estudiantiles, discos duros internos.

Fuente: Autoría propia

2.3.4 Evidencias Fotográficas de los recursos informáticos en la IEM Ciudad de Pasto

Esta sección presenta y describe evidencia fotográfica que respalda la evaluación de los recursos informáticos en la IEM Ciudad de Pasto, en las imágenes obtenidas durante el trabajo de campo de la investigación se puede observar la infraestructura tecnológica del plantel, el entorno de aprendizaje en el área de tecnología e informática, el estado de las redes de internet, la interacción de la tecnología en la función de cada una de las áreas de la institución y otros aspectos que se han ido explicando en las descripciones de las áreas y su respectivo inventario.

2.3.5 Evidencia fotográfica aulas de Informática

Imagen No. 1 *Aula informática # 1*

Fuente: Bravo, C.A., (2023). Fotografía aula de informática # 1 [JPG]. Localizada en la Institución Educativa Municipal Ciudad de Pasto, San Juan de Pasto – Nariño- Colombia, 2023.

Imagen No. 2 *Aula informática # 1*

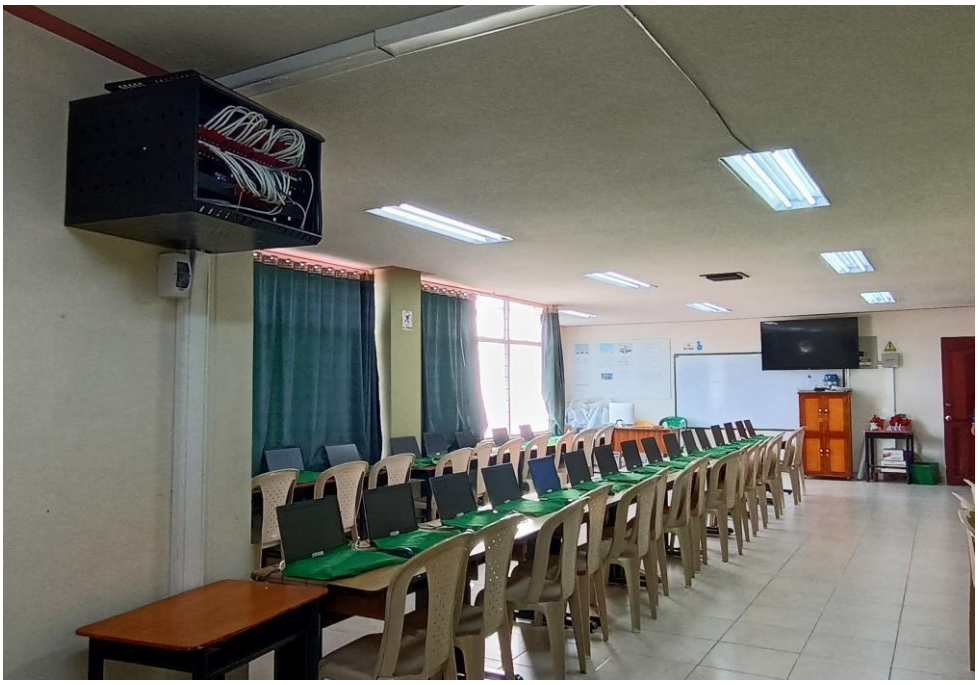
Fuente: Bravo, C.A., (2023). Fotografía aula de informática # 1 [JPG]. Localizada en la Institución Educativa Municipal Ciudad de Pasto, San Juan de Pasto – Nariño- Colombia, 2023.

Imagen No. 3 *Aula informática # 1*

Fuente: Bravo, C.A., (2023). Fotografía aula de informática # 1 [JPG]. Localizada en la Institución Educativa Municipal Ciudad de Pasto, San Juan de Pasto – Nariño Colombia.

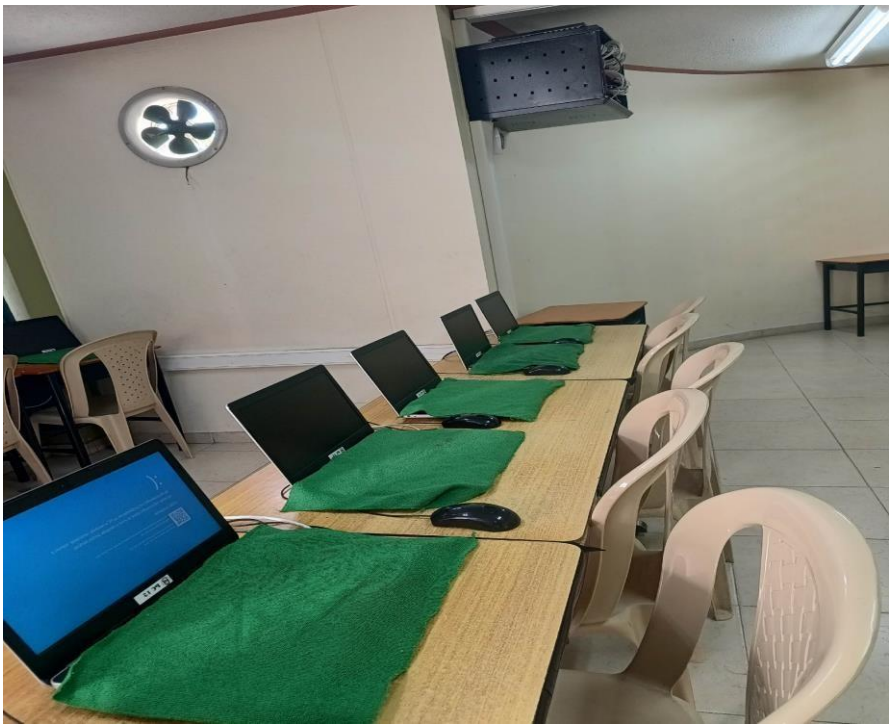
Las imágenes 1, 2 y 3 muestran el aula informática No. 1 de la IEM Ciudad de Pasto, cuenta con 40 equipos portátiles, cada uno con su toma corriente, cargador, cable de conexión a red, mouse, mesa y silla, un equipo de escritorio el cual es de uso exclusivo del docente, un TV SMART usado para compartir pantalla para las actividades académicas pertinentes y un tablero.

Imagen No. 4 *Aula informática # 2*



Fuente: Bravo, C.A., (2023). Fotografía aula de informática # 2 [JPG]. Localizada en la Institución Educativa Municipal Ciudad de Pasto, San Juan de Pasto – Nariño, Colombia.

Imagen No. 5 *Aula informática # 2*



Fuente: Bravo, C.A., (2023). Fotografía aula de informática # 2 [JPG]. Localizada en la Institución Educativa Municipal Ciudad de Pasto, San Juan de Pasto – Nariño Colombia.

Las imágenes 4 y 5 muestran el aula informática No. 2 de la IEM Ciudad de Pasto, cuenta con 40 equipos portátiles, cada uno con su toma corriente, cargador, cable de conexión a red, mouse, protector de teclado, mesa y silla, un equipo de escritorio el cual es de uso exclusivo del docente, un TV SMART usado para compartir pantalla para las actividades académicas pertinentes y un tablero, cuenta con su respectivo rotures y cableado.

Imagen No. 6 *Aula informática # 3*

Fuente: Bravo, C.A., (2023). Fotografía aula de informática # 3 [JPG]. Localizada en la Institución Educativa Municipal Ciudad de Pasto, San Juan de Pasto – Nariño, Colombia, 2023.

Imagen No. 7 *Aula informática # 3*

Fuente: Bravo, C.A., (2023). Fotografía aula de informática # 3 [JPG]. Localizada en la Institución Educativa Municipal Ciudad de Pasto, San Juan de Pasto – Nariño, Colombia, 2023

Las imágenes 6 y 7 muestran el aula informática No. 3 de la IEM Ciudad de Pasto, cuenta con 13 equipos portátiles, cada uno con su toma corriente, cargador, cable de conexión a red, mouse, mesa y silla, 28 equipos de escritorio, uno de ellos es de uso exclusivo del docente, un TV SMART usado para compartir pantalla para las actividades académicas pertinentes y un tablero.

Imagen No. 8 *Aula informática Galileo*

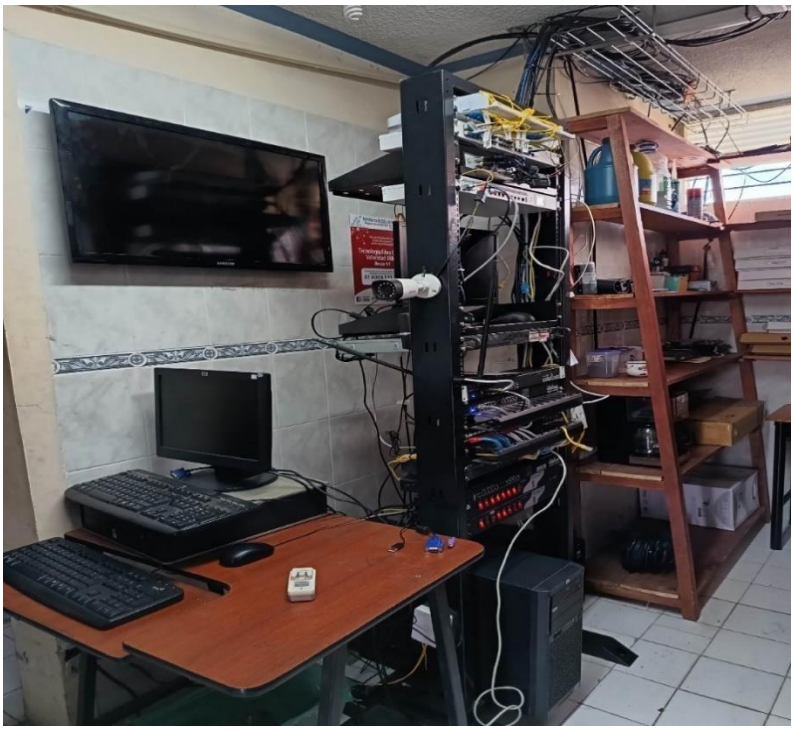
Fuente: Bravo, C.A., (2023). Fotografía aula de informática Galileo [JPG]. Localizada en la Institución Educativa Municipal Ciudad de Pasto, San Juan de Pasto – Nariño, Colombia, 2023

Imagen No. 9 *Aula informática Galileo*

Fuente: Bravo, C.A., (2023). Fotografía aula de informática Galileo [JPG]. Localizada en la Institución Educativa Municipal Ciudad de Pasto, San Juan de Pasto – Nariño, Colombia, 2023

Las imágenes 8 y 9 muestran el aula informática Galileo de la IEM Ciudad de Pasto, cuenta con 40 equipos portátiles, cada uno con su toma corriente, cargador, cable de conexión a red, mouse, protector de teclado, mesa y silla, un equipo de escritorio el cual es de uso exclusivo del docente, un TV SMART usado para compartir pantalla para las actividades académicas pertinentes y un tablero, cuenta con su respectivo rotures y cableado.

Imagen No. 10 *Oficina de Ingeniería y recursos tecnológicos*



Fuente: Bravo, C.A., (2023). Fotografía Oficina de Ingeniería y recursos tecnológicos [JPG]. Localizada en la Institución Educativa Municipal Ciudad de Pasto, San Juan de Pasto – Nariño, Colombia, 2023.

Imagen No. 11 ***Oficina de Ingeniería y recursos tecnológicos.***

Fuente: Bravo, C.A., (2023). Fotografía Oficina de Ingeniería y recursos tecnológicos [JPG]. Localizada en la Institución Educativa Municipal Ciudad de Pasto, San Juan de Pasto – Nariño Colombia, 2023.

La oficina de ingeniería es la encargada de supervisar y estar al pendiente de los equipos y redes institucionales, como se puede ver en las imágenes 11 y 12 la oficina cuenta con un computador de escritorio, un TV, router, switches y los servidores de la institución, también se puede observar la red LAN.

2.4 Vulnerabilidades, Riesgos y Amenazas en la IEM Ciudad de Pasto

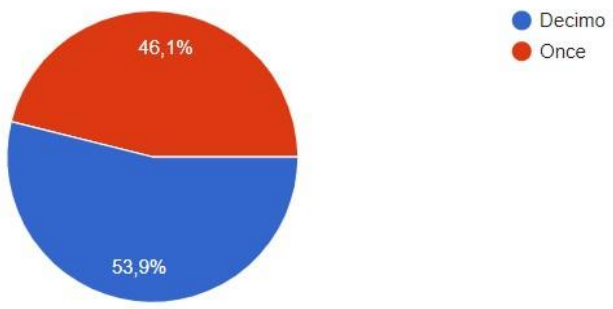
Para determinar las vulnerabilidades, riesgos y amenazas en los sistemas informáticos en la IEM Ciudad de Pasto, se realizó el trabajo de campo mediante una encuesta en el año 2023 para recolectar

la información pertinente sobre los riesgos a los que se enfrentan los estudiantes en internet y la orientación que reciben para manejar estas situaciones, la encuesta fue dirigida a 323 estudiantes de los grados decimos y once, después de la aplicación del instrumento se obtienen los siguientes datos:

Pregunta 1. ¿Qué grado está cursando?

Figura 5

Grados encuestados



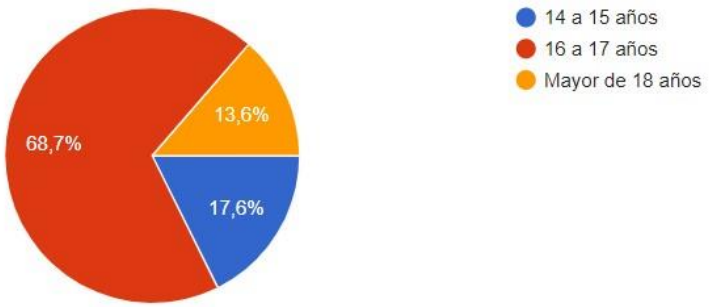
*L*a figura 5 muestra la división de la población estudiantil según el grado que cursa en la IEM ciudad de Pasto en Nariño - Colombia en el año 2023.

Los 323 jóvenes encuestados corresponden a estudiantes que cursan grado decimo y once y se dividen de la siguiente manera, el 46% están cursando el grado 11 correspondiente a 174 estudiantes y un 53% de grado decimo correspondiente a 149 estudiantes según la muestra.

Pregunta 2. ¿Edad de los estudiantes encuestados?

Figura 6

Edades encuestadas

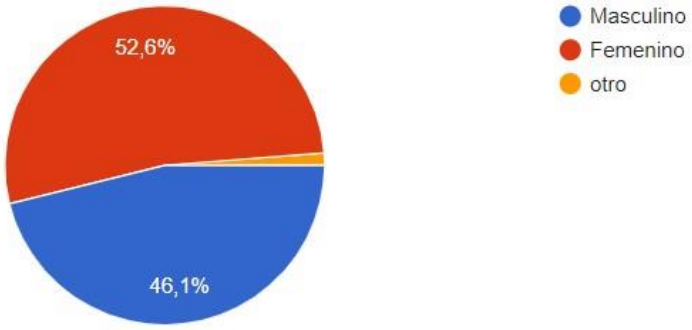


La figura 6 muestra La división de los jóvenes encuestados por intervalos de edad, el mayor porcentaje de estudiantes se encuentran entre los 16 - 17 años con un 68.7% seguida de 14 - 15 años que lo representa un 17.6% de la población y un 13.6% es representada por jóvenes que ya cumplieron la mayoría de edad.

Pregunta 3. ¿Género de los estudiantes encuestados?

Figura 7

Géneros Encuestados



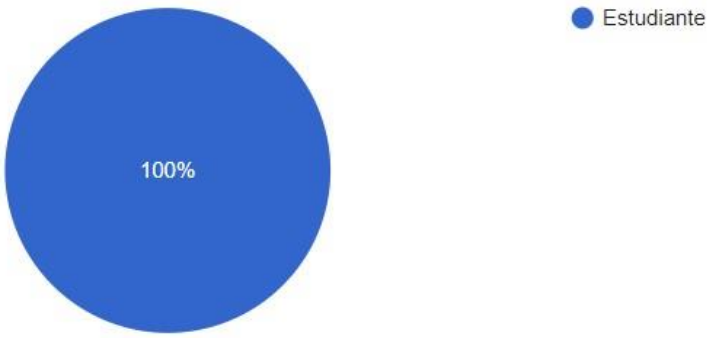
La figura 7 muestra la división de estudiantes objeto de investigación por género, un 52.6% de los estudiantes se identifican con el género femenino, seguido del 46.1% que se identifican con el género

masculino y un porcentaje mínimo de 1.3% que no se identifican en estos grupos mencionados anteriormente.

Pregunta 4. ¿Rol?

Figura 8

Roles

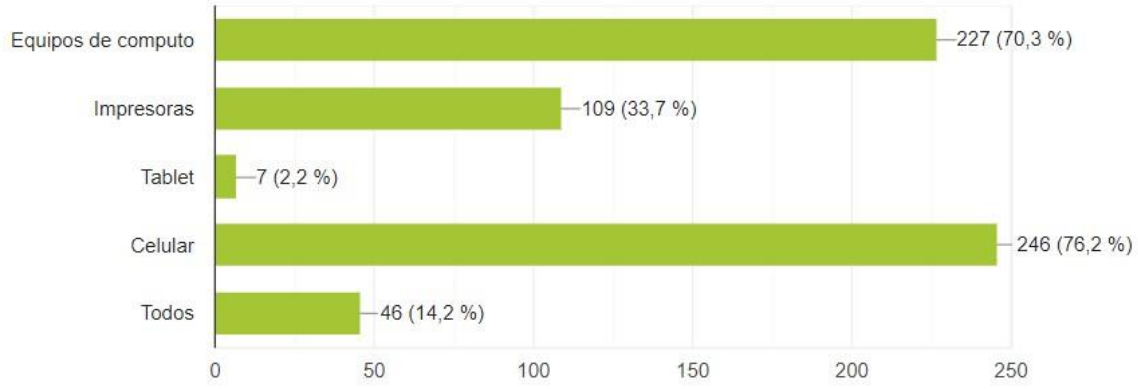


La figura 8 nos muestra que el 100% de los jóvenes encuestados son estudiantes de la IEM Ciudad de Pasto

Pregunta 5. ¿Qué dispositivos tecnológicos utiliza regularmente en sus actividades escolares o académicas?

Figura 9

Distribución del Uso de Dispositivos Tecnológicos

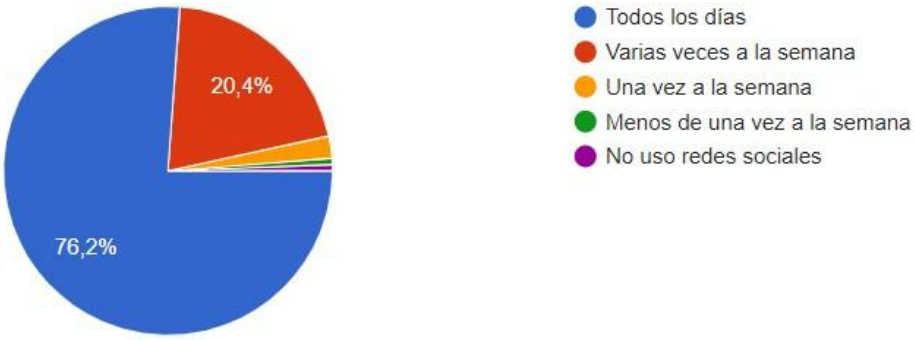


En la figura 9 se puede observar cual es el dispositivo tecnológico más usado por los estudiantes, esta pregunta es de opción múltiple y los datos arrojan que el uso del celular es el más frecuente con 246 estudiantes eligiendo esta opción, seguido de equipos de cómputo que lo representa 227 estudiantes, impresoras con 109 estudiantes, todos los anteriores con 46 estudiantes y la opción menos repetida fue Tablet con 7 estudiantes.

Pregunta 6. ¿Con qué frecuencia utilizas las redes sociales?

Figura 10

Frecuencia uso de Redes sociales



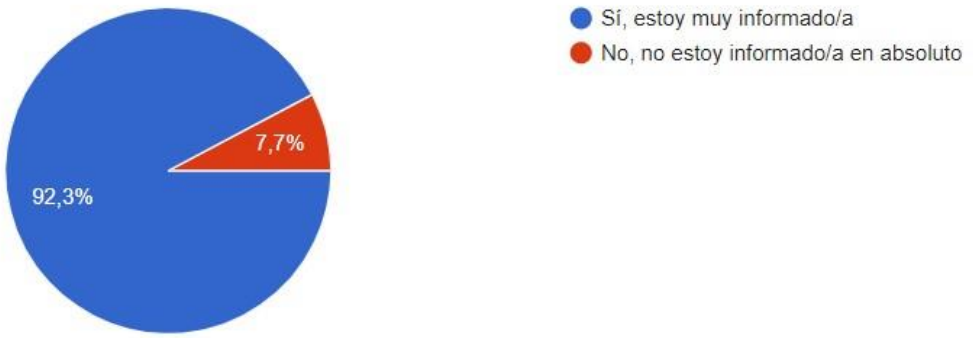
En la figura 10 se muestra las gráficas de frecuencia para uso de redes sociales podemos observar que los estudiantes mantienen una vida activa en redes sociales, el 76.2% de los estudiantes

encuestados afirman que utilizan redes sociales todos los días, un 20.4% lo hacen varias veces a la semana y solo un 3.4% revisan sus redes una vez a la semana o con menos intensidad, todos los estudiantes encuestados tienen redes sociales y están activos en ellas.

Pregunta 7. ¿Estás al tanto de las posibles amenazas y vulnerabilidades en las redes sociales?

Figura 11

Nivel de Información de los Usuarios

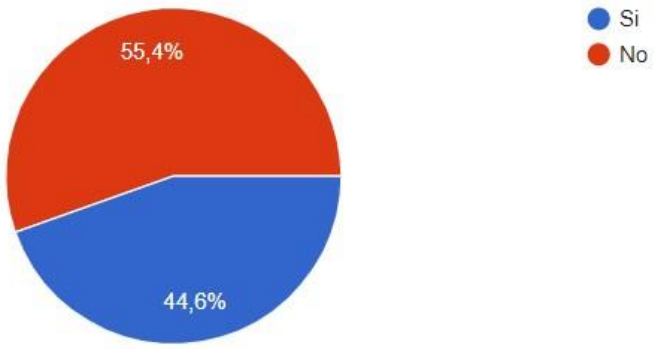


En la Figura 11 se muestra la consciencia de los jóvenes encuestados frente a las posibles amenazas y vulnerabilidad de redes sociales, un 92.7% de los estudiantes están conscientes de los peligros que corren en las redes sociales y solo un 7.3% no conocen las amenazas que enfrentan.

Pregunta 8. ¿Has experimentado alguna vez una vulnerabilidad o amenaza en tus perfiles de redes sociales? Por ejemplo, hackeo de cuenta, suplantación de identidad, acoso en línea, etc.

Figura 12

Experiencias de Vulnerabilidad en Redes Sociales

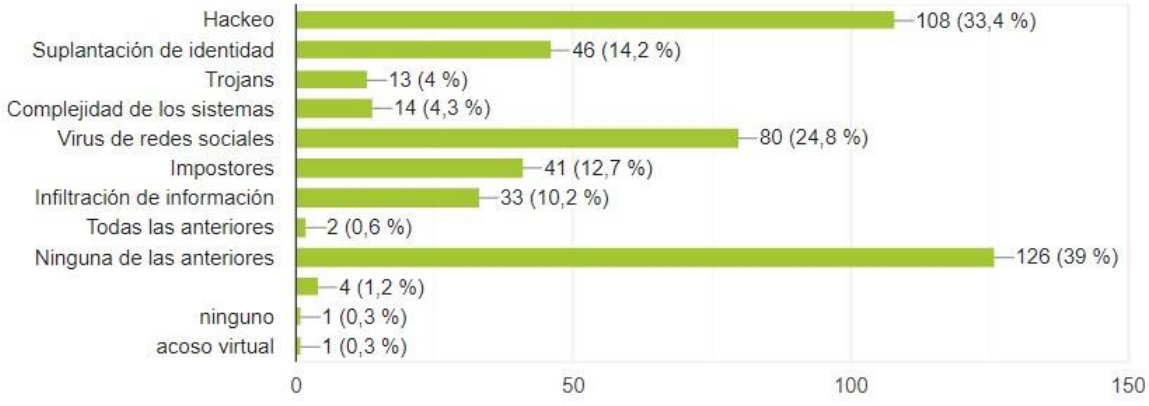


En la Figura 12 se muestra el porcentaje de estudiante que se han experimentado alguna vulnerabilidad en redes sociales, según las respuestas dadas el 55.4% no ha sufrido ninguna vulnerabilidad o amenaza en redes sociales mientas que el 44.6% si ha experimentado alguna amenaza

Pregunta 9. ¿En caso de que "SI" cuál de los siguientes tipos de vulnerabilidades ha tenido?

Figura 13

Vulnerabilidades más frecuentes

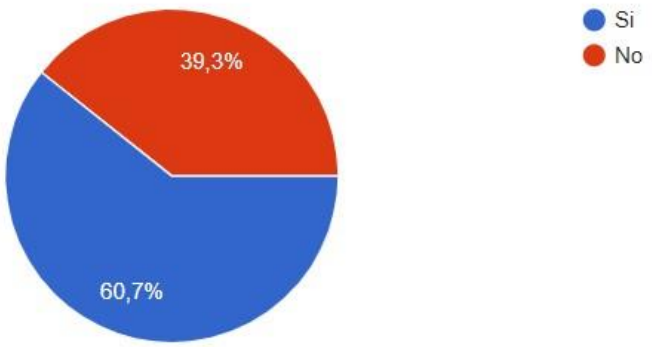


En la figura 13 se muestra La vulnerabilidad que más han presentado los estudiantes, esta pregunta es de opción múltiple, 126 estudiantes no han presentado ningún caso de vulnerabilidad en redes, la vulnerabilidad que más se ha repetido es el hackeo de redes sociales con 108 casos, seguido de virus de redes sociales con 80 casos, suplantación de identidad 46 casos, impostores 41 casos, infiltración de información 33 casos, las vulnerabilidades con menos incidencia son complejidad de sistemas con 14 casos, trojans 13 casos, todas las anteriores 2 casos y acoso virtual con 1 caso

Pregunta 10. ¿En las aulas de informática los equipos de cómputo poseen antivirus?

Figura 14

Antivirus en aulas de informática

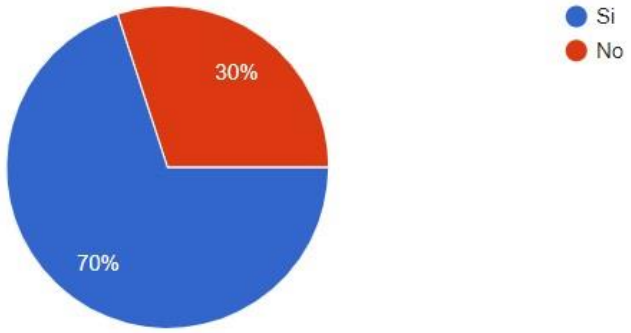


En la figura 14 según la repuesta de los estudiantes se muestra que el 60.8% responden que los equipos de las aulas de informática si poseen antivirus, mientras que el 39.3% aseguran que no, para este ejercicio los estudiantes buscaron en el computador el antivirus y posterior respondieron.

Pregunta 11. ¿Si existen antivirus, las aulas de informática los equipos de cómputo estos antivirus están actualizados?

Figura 15

Antivirus actualizados

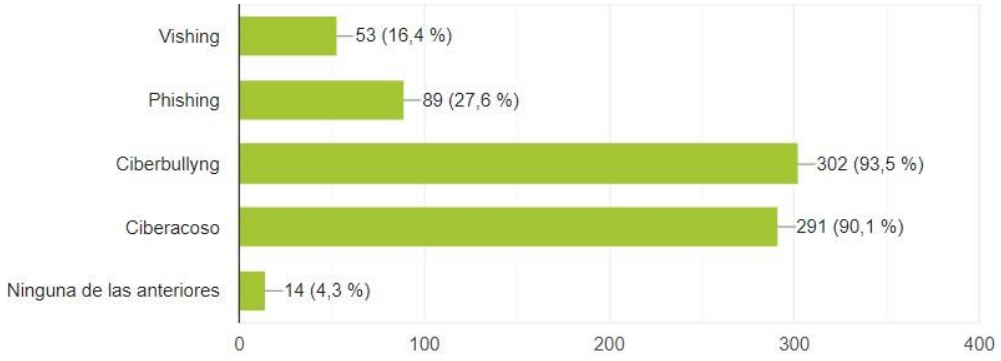


En la figura 15 se muestra que un 70% de los estudiantes encuestados afirman que los antivirus de los equipos si están actualizados y un 30% responden que no. Para este ejercicio los estudiantes buscaron en el computador el antivirus y posterior respondieron

Pregunta 12. ¿De los siguientes que tipos de delitos informáticos conoce?

Figura 16

Conocimientos de delitos informáticos



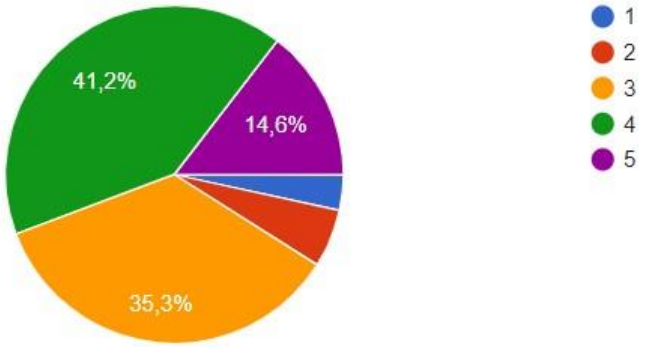
En la figura 16 se muestra los tipos de delitos informáticos que más conocen los estudiantes, esta pregunta es de respuesta múltiple y arroja que los delitos informáticos más conocidos son el ciberbullying con 302 respuestas y el ciberacoso 291 respuestas. Lo siguen delitos como phishing

con 89 respuestas y vishing con 53 respuestas, la opción menos seleccionada fue ninguna de las anteriores con 14 estudiantes.

Pregunta 13. Califique de 1 a 5 el nivel de seguridad de la información en sus equipos de cómputo (nivel 1 más bajo y nivel 5 el más alto)

Figura 17

Seguridad de la información



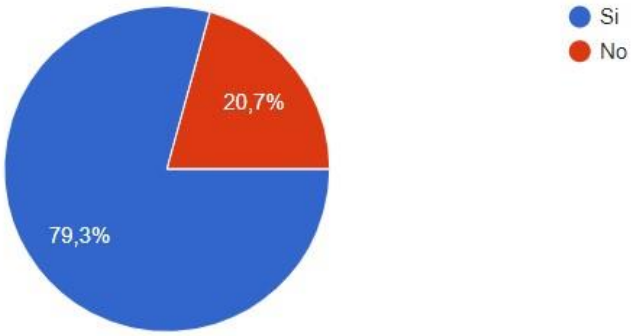
En la figura 17 muestra el nivel de seguridad que los estudiantes observan en los equipos de cómputo, el 41.2% de los estudiantes afirman que el nivel de seguridad es bueno, el 35.3% afirman que es intermedio y el 14.6% dicen que es excelente.

Las opciones menos seleccionadas fueron 1 y 2 que representan un nivel de seguridad malo y muy malo.

Pregunta 14. ¿Tiene usted conocimiento acerca de delitos informáticos o de las vulnerabilidades de seguridad?

Figura 18

Conocimiento de vulnerabilidades de seguridad

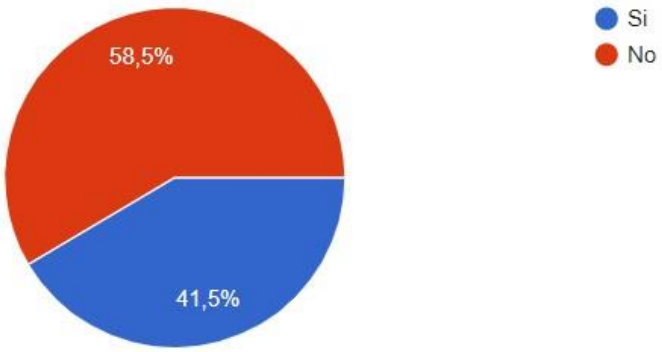


La figura 18 muestra que el 79.3% de los estudiantes encuestados afirman tener conocimiento sobre delitos y vulnerabilidades informáticas y solo el 20.7% afirman no tener ningún tipo de información

Pregunta 15. ¿Ha tenido capacitación en delitos informáticos por parte de la Institución?

Figura 19

Capacitación de la Institución

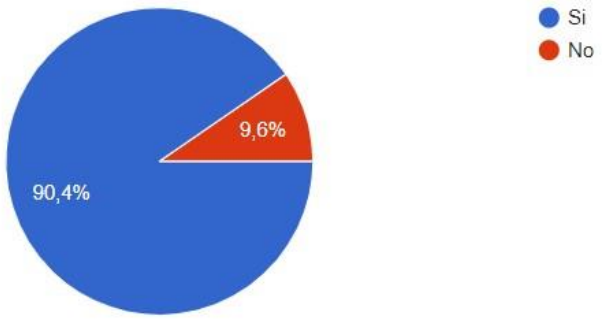


La figura 19 muestra que el 58.5% de los estudiantes consultados afirman no tener ninguna capacitados en delitos informáticos por parte de la institución, mientras que el 41.5% afirman que si han tenido la oportunidad de ser capacitados.

Pregunta 16. ¿Conoce las plataformas virtuales que dispone la institución para su trabajo académico?

Figura 20

Conocimiento de plataformas virtuales

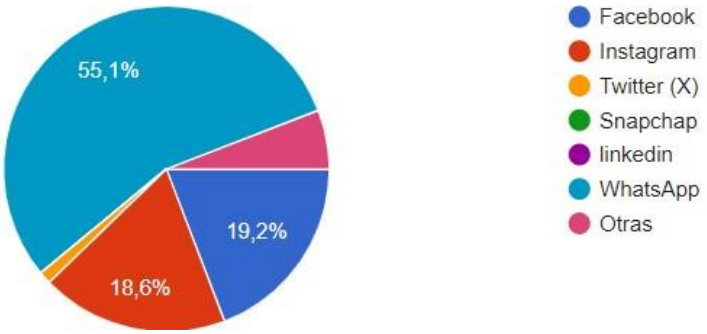


La figura 20 muestra que el 90.4% tienen de los estudiantes tienen conocimiento que las plataformas virtuales con las que la institución cuenta para el desarrollo de las actividades académica

Pregunta 17. De las siguientes redes sociales. ¿Cuál usa usted utiliza con más frecuencia?

Figura 21

Frecuencia en redes sociales

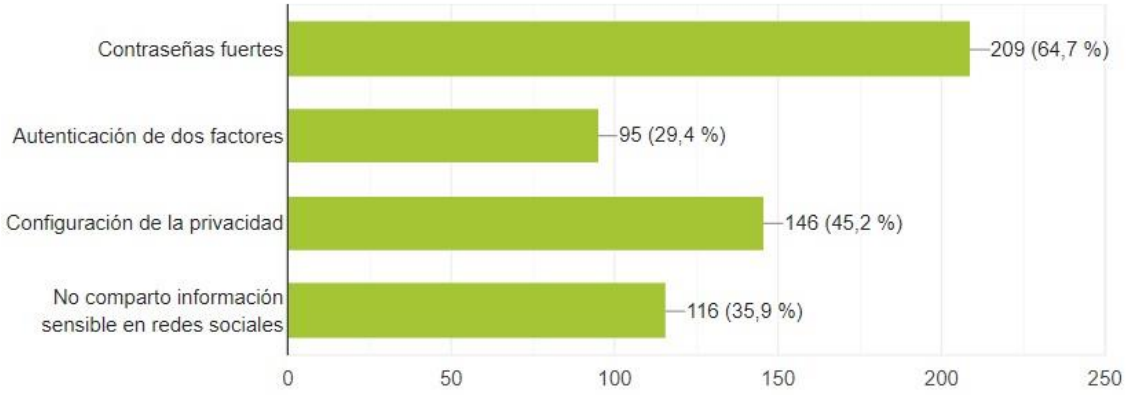


La figura 21 muestra que La red social más usada por los estudiantes es WhatsApp con un 55,1%, seguida de Facebook con un porcentaje de 19,2%, Instagram con 18,2%, las opciones menos seleccionadas fueron otras redes sociales con un 5,9%y twitter con un 1,2 %, Snapchat y LinkedIn no tuvieron ninguna representación.

Pregunta 18. ¿Qué medidas de seguridad utilizas para proteger tu información en las redes sociales? (Selecciona todas las que correspondan)

Figura 22

Medidas de protección en redes sociales

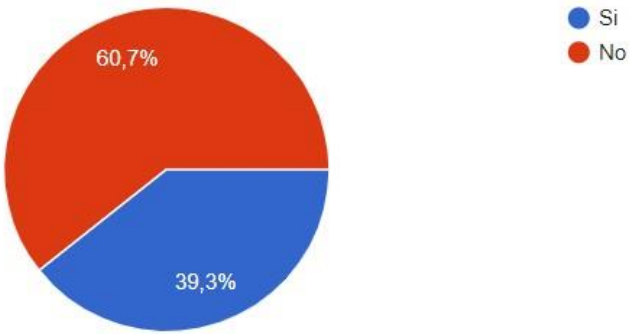


La figura 22 muestra las medidas de seguridad que toman los estudiantes para protegerse en la red, esta pregunta es de respuesta múltiple y arroja que el método más utilizado para proteger información por parte de los estudiantes es contraseñas fuertes con 209 respuestas, seguido de configuración de privacidad con 146 respuestas, no compartir información sensible 116 respuestas y la opción menos utilizada es la autenticación en dos factores con 95 casos.

Pregunta 19. ¿Alguna vez has compartido información personal sensible, como números de teléfono, direcciones, o detalles de identificación en las redes sociales?

Figura 23

Información personal compartida

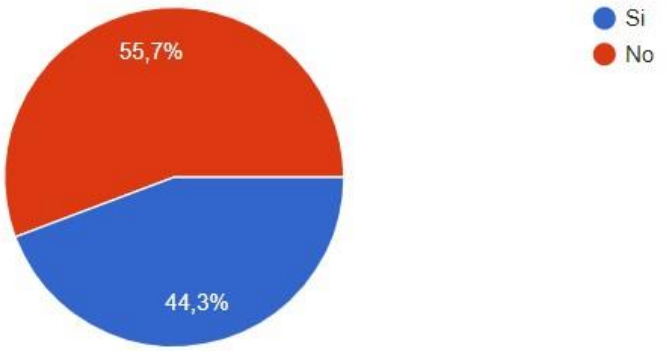


En la figura 23 se muestra que el 60.7% de los estudiantes encuestados afirman que no han publicado datos sensibles o de información personal en sus redes sociales y el 39.3% si lo han hecho

Pregunta 20. ¿Conoce usted que en la institución cuenta con políticas claras de seguridad informática en el uso de las redes sociales?

Figura 24

Conocimiento de políticas de seguridad informática

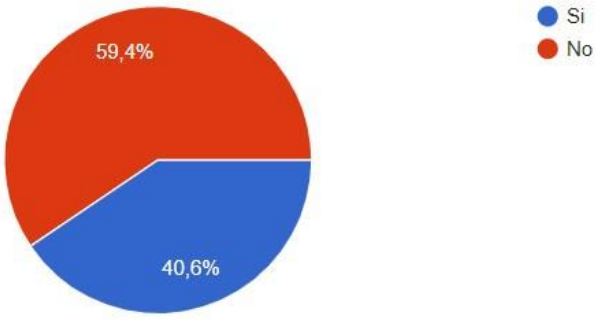


En la figura 24 se muestra que el 56.7% de los estudiantes encuestados las políticas de seguridad informática de la institución son desconocidas y el 44.3% afirma si tener conocimiento sobre las mismas.

Pregunta 21. ¿Existe una ruta en la institución para el manejo de casos de vulnerabilidad en sistemas informáticos?

Figura 25

Casos de vulnerabilidades

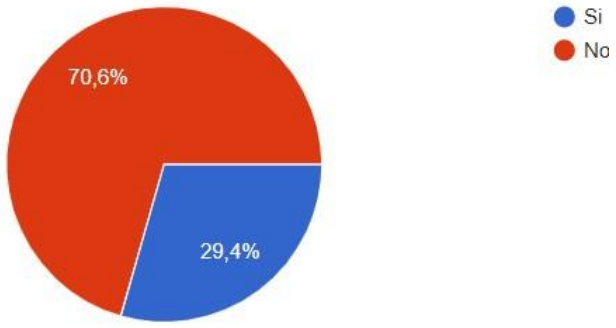


En la figura 25 se muestra que el 59.4% de los estudiantes afirman que no conocen la ruta de manejo que tiene la institución para atender casos de vulnerabilidad en sistemas informáticos, mientras que el 44.3% si las conocen.

Pregunta 22. ¿Conoce usted que la institución monitorea las interacciones en las redes sociales para identificar posibles signos de vulnerabilidad entre los estudiantes?

Figura 26

Interacciones en redes sociales

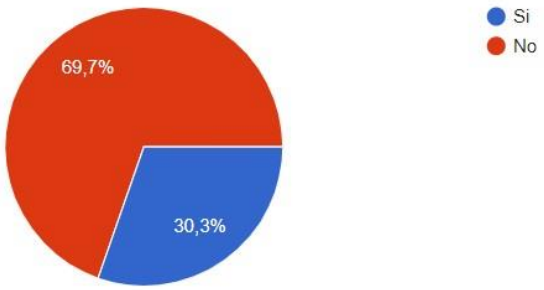


En la figura 26 se muestra que el 70.6% de los estudiantes encuestados no conocían que la institución tiene un monitoreo de redes sociales para identificar signos de vulnerabilidad entre los estudiantes. Y solo un 29.4% tenían conocimiento de esta información.

Pregunta 23. ¿Conoce usted si la institución ha intervenido en algún caso en el que hayan intervenido debido a una situación de vulnerabilidad que se haya manifestado por el uso de las redes sociales?

Figura 27

Intervención Institucional en Casos de Vulnerabilidad

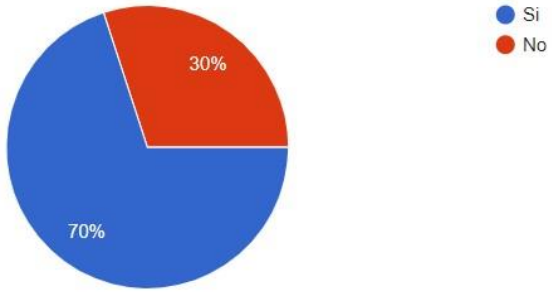


En la figura 27 se muestra que los estudiantes encuestados 69,7% afirman que no ha intervenido la institución para mitigar los riesgos, mientras el 30,3% dicen que si han sido intervenidos.

Pregunta 24. ¿La institución promueve el uso responsable y ético de las redes sociales entre los estudiantes para evitar situaciones de vulnerabilidad?

Figura 28

Promueve el uso responsable de redes sociales

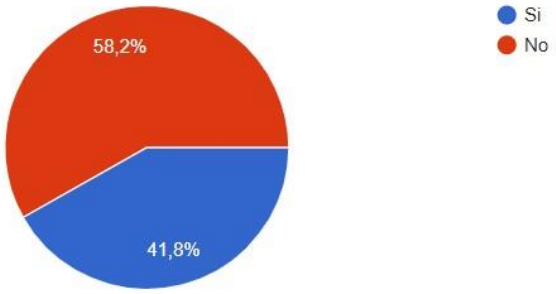


En la figura 28 se muestra que los estudiantes encuestados un 70% afirman que la institución ayuda a promover el uso responsable de redes sociales y así evitar que sus estudiantes estén expuestos.

Pregunta 25. ¿La institución ofrece orientación o recursos en línea para ayudar a ustedes los estudiantes a lidiar con problemas de vulnerabilidad que puedan surgir en redes sociales?

Figura 29

Orientación y recursos

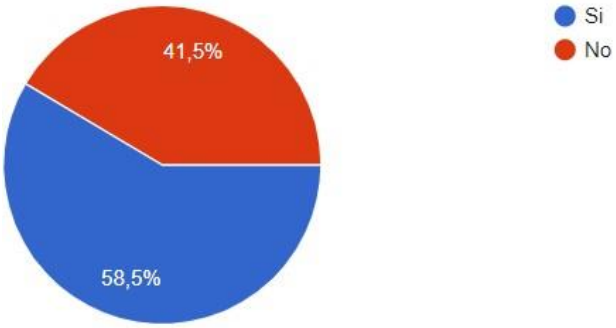


En la figura 29 se muestra que el 58.2% de la población encuestada afirmar que la institución no ofrece orientación o recursos en línea para atender casos de vulneración en redes sociales de los estudiantes y el 42.8% afirman que la institución si cuenta con este servicio

Pregunta 26. ¿La institución capacita a ustedes los estudiantes sobre la importancia de la privacidad y la seguridad en línea para prevenir situaciones de vulnerabilidad?

Figura 30

Prevención de situaciones de vulnerabilidad

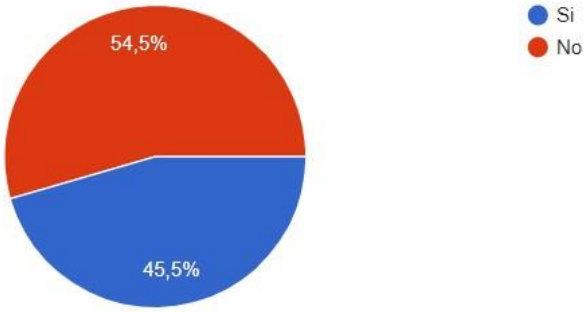


En la figura 30 se muestra que el 58.5% de los estudiantes encuestados afirman que la institución si los capacita para conocer la importancia de la privacidad y el buen manejo de la información. Y el 41.5% de los estudiantes afirman que no han sido capacitados por la institución en esta área

Pregunta 27. ¿Conoce si la institución fomenta la denuncia de situaciones de vulnerabilidad en redes sociales y se brinda una ruta para hacerlo de manera segura?

Figura 31

Denuncia de situaciones de vulnerabilidad

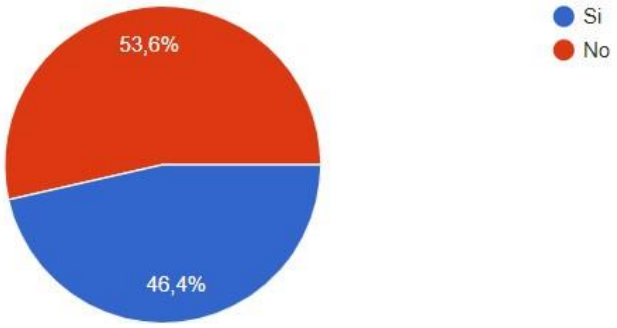


En la figura 31 se muestra que el 54.5% de los estudiantes dicen no conocer si la institución fomenta la denuncias para situaciones de vulnerabilidad en redes sociales y el 45.5% afirman que si tener información respecto al tema.

Pregunta 28. ¿Conoce si en la institución las medidas de seguridad básicas para proteger tus cuentas en redes sociales, como el uso de contraseñas fuertes o la autenticación de dos factores?

Figura 32

Conocimiento de medidas de seguridad

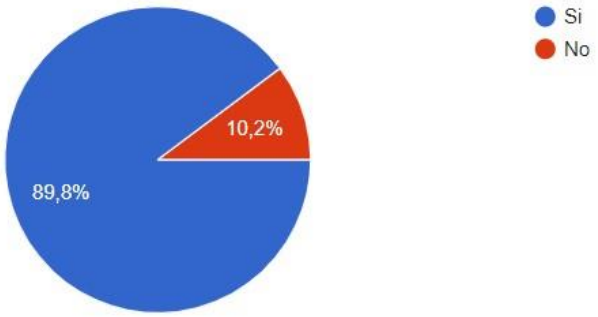


En la figura 32 se muesra que el 53.6% de los estudiantes dicen no conoce las medidas básicas de seguridad y el 46.4% afirman que si tener conocimiento de la institución.

Pregunta 29. ¿Has recibido solicitudes de amistad o seguidores de personas desconocidas en tus redes sociales?

Figura 33

Interacción con personas desconocidas

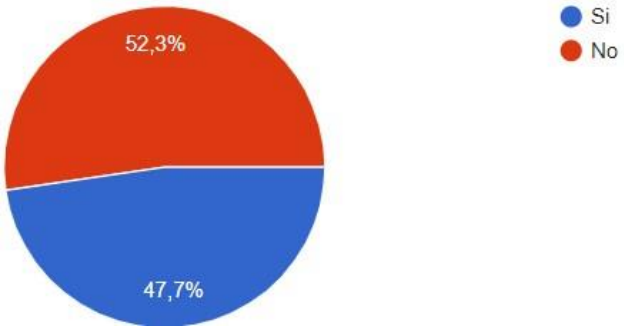


En la figura 33 se muestra que el 89.8% de los estudiantes encuestados afirman que en algún momento han recibidos solicitudes de amistades de personas extrañas en redes sociales y el 10.2% no lo han hecho

Pregunta 30. ¿Has notado un aumento en el acoso en línea o en la divulgación de información personal de otros estudiantes en las redes sociales?

Figura 34

Aumento en el acoso en línea

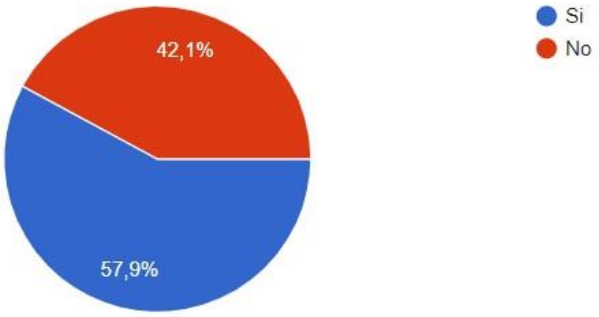


El 52.3% de los estudiantes no han notado un aumento en el acoso o divulgación de información sensible por parte de los estudiantes, el 47.7% de los estudiantes si han percibido situaciones de este tipo.

Pregunta 31. ¿Te sientes cómodo/a denunciando situaciones de acoso o vulnerabilidades en tus redes sociales a las autoridades escolares o a los administradores de la plataforma?

Figura 35

Situaciones de denuncias

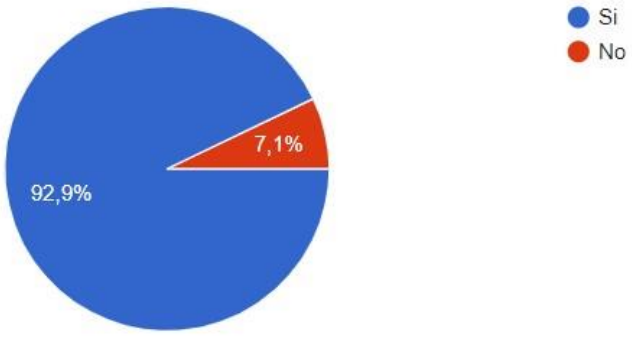


Frente a la pregunta sobre comodidad a la hora de denunciar un caso de vulnerabilidad en redes sociales ante la institución el 57.9% de los estudiantes si sienten comodidad al hacerlo y el 42.1% no tiene ninguna vulnerabilidad.

Pregunta 32. ¿Crees que tu colegio debería proporcionar más educación sobre seguridad en línea y protección de datos a los estudiantes?

Figura 36

Educación sobre seguridad

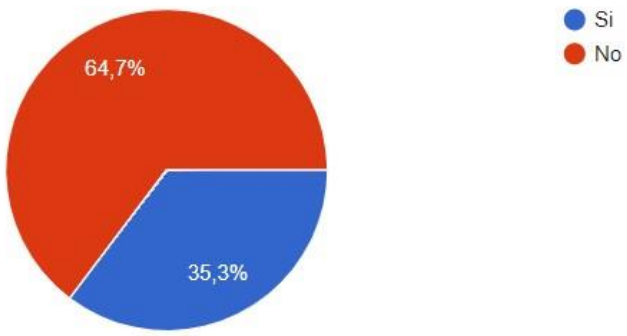


El 92.9% de los estudiantes están de acuerdo en poder recibir educación y capacitación para poder estar seguros en línea y tener protección de datos.

Pregunta 33. ¿Alguna vez has compartido imágenes o contenido en redes sociales que más tarde te arrepentiste de haber compartido?

Figura 37

Contenido compartido en redes sociales



El 64.7% de los estudiantes no han subido a sus redes contenido del cual sufran arrepentimiento de subirlo, y el 35.3% si lo han hecho en algún momento.

Después de analizar detalladamente los resultados de la encuesta realizada a los estudiantes de la IEM Ciudad de Pasto en relación con los riesgos y la orientación para el manejo de casos relacionados con ciberataques, se concluye lo siguiente:

- Consciencia de riesgos en redes sociales: La gran mayoría de los estudiantes encuestados están conscientes de los peligros y vulnerabilidades que enfrentan en las redes sociales, lo que indica un nivel básico de educación sobre seguridad en línea.
- Experiencia de vulnerabilidades: Aunque una parte significativa de los estudiantes ha experimentado vulnerabilidades en sus perfiles de redes sociales, como el hackeo de cuentas o la suplantación de identidad, también es alentador ver que muchos de ellos aún no han enfrentado tales situaciones.
- Medidas de seguridad: Los estudiantes muestran una inclinación hacia la adopción de medidas de seguridad básicas, como el uso de contraseñas fuertes y la configuración de la privacidad en sus perfiles de redes sociales. Sin embargo, todavía hay áreas de mejora, como la implementación de la autenticación de dos factores.
- Educación y capacitación: Aunque una proporción considerable de estudiantes afirma haber recibido capacitación sobre delitos informáticos y seguridad en línea por parte de la institución, también hay un número significativo que no ha tenido acceso a este tipo de

formación. Esto destaca la necesidad de una mayor difusión y disponibilidad de programas educativos sobre seguridad digital.

- Conocimiento institucional: Existe una falta de conocimiento entre los estudiantes sobre las políticas de seguridad informática y los procedimientos para el manejo de casos de vulnerabilidad en sistemas informáticos implementados por la institución. Esto indica la necesidad de una mejor comunicación y transparencia por parte de la institución en relación con estas cuestiones.
- Disposición a denunciar casos: A pesar de que una parte significativa de los estudiantes se siente cómoda denunciando casos de acoso o vulnerabilidad en redes sociales a las autoridades escolares, aún existe una proporción considerable que no se siente cómoda haciendo tales denuncias. Esto resalta la importancia de crear un entorno seguro y de confianza para que los estudiantes puedan reportar incidentes de manera efectiva.

Si bien los estudiantes muestran cierto nivel de conciencia y prácticas de seguridad en línea, todavía hay áreas de mejora tanto a nivel individual como institucional. Se requiere una mayor educación y capacitación en seguridad digital, así como una mejor comunicación y apoyo por parte de la institución para garantizar la protección adecuada de los estudiantes en el entorno en línea.

Con el análisis de datos de los instrumentos aplicados se procede a construir la matriz de riesgos y amenazas desde la metodología Magerit.

2.4.1 Matrices de riesgos y amenazas Magerit

A continuación, se presentan matrices de riesgos y amenazas que han sido identificados en las redes informáticas de la IEM Ciudad de Pasto, junto con su probabilidad de ocurrencia y el impacto potencial en la institución:

14. Protección de equipos contra hackers, virus y amenazas internas y externas.

15. Amenazas contra privacidad de los estudiantes en redes sociales.

16. Prevención y orientación por parte de la institución para manejo de casos relacionados con ciberataques.

17. Delito informáticos presentados en la institución educativa.

Estas matrices ofrecen una visión general de las principales amenazas y riesgos a los que se enfrenta las redes sociales de la IEM Ciudad de Pasto, destacando la probabilidad de ocurrencia y el impacto potencial de cada uno. Es fundamental para la institución tomar medidas proactivas para mitigar estos riesgos y proteger la integridad, confidencialidad y disponibilidad de sus sistemas informáticos.

Tabla 14

Clasificación del riesgo

FR (frecuencia) Improbable (I) Poco probable (PP) Probable (P) Muy Probable (MP)
INT (intensidad) Baja (B) Media(M) Alta(A) Muy Alta (MA)
COB (cobertura) Poca (P) Media (M) Alta (A) Total (T)

Tabla 15

Matriz de evaluación de seguridad informática

Situación	Procesos de riesgo	Activos afectados	Caracterizacion / Calificacion			
			Fr	Int	Cob	Gama de color
Protección de equipos contra hackeos, virus, amenazas internas y externas.	La institución cuenta con red de antivirus.	Red de área local (LAN)	I	B	P	ALTO
	Conocimiento de los estudiantes sobre la protección que poseen los equipos informáticos en la institución.	Equipos informáticos	P	M	M	MEDIO
	Nivel de seguridad de los equipos de cómputo usado por los estudiantes	Equipos informáticos	P	A	A	BAJO

Tabla 16

Matriz de amenazas por redes sociales

Situación	Procesos de riesgo	Activos afectados	Caracterización / Calificación			
			Fr	Int	Cob	Gama de Color
Amenazas contra privacidad de los estudiantes en redes sociales.	Frecuencia con la cual se utiliza redes sociales.	Datos y acceso credenciales	M.P	M.A	A	ALTO
	Nivel de protección de la información publicada en redes sociales.	Datos y acceso credenciales	M.P	M.A	A	BAJO
	Conocimiento sobre riesgos y vulnerabilidades a los que se expone en redes sociales.	Datos y acceso credenciales	P	M	M	MEDIO

Situación	Procesos de riesgo	Activos afectados	Caracterización / Calificación			
			Fr	Int	Cob	Gama de Color
	Riesgos o vulnerabilidad en perfiles y redes sociales.	Datos y acceso credenciales	M.P	M.A	T	BAJO
	Medidas de seguridad para proteger las redes sociales.	Datos y acceso credenciales	P.P	M	B	BAJO
	Información personal sensible compartida en alguna red social.	Datos y acceso credenciales	M.P	A	A	ALTO
	Ataques y vulnerabilidades de personas desconocidas en redes sociales.	Datos y acceso credenciales	P	M	M	MEDIO
	Se nota aumento en el acoso a estudiantes por información divulgada en redes sociales.	Datos y acceso credenciales				

Tabla 17

Matriz de conocimiento de casos de ciberataques

Situación	Procesos de riesgo	Activos Afectados	Caracterización / Calificación			
			Fr	Int	Cob	Gama de color
Prevención y orientación por parte de la institución para manejo de casos relacionados con ciberataques.	Conocimiento de las políticas de seguridad informática por parte de la institución.	Datos y acceso credenciales	P	M	M	MEDIO
	Conocimiento de la ruta a seguir por la institución en caso de presentar casos de vulnerabilidad en sistemas informáticos	Datos y acceso credenciales	P	M	M	MEDIO
		Datos y acceso credenciales	P.P	B	B	ALTO

Situación	Procesos de riesgo	Activos Afectados	Caracterización / Calificación			
			Fr	Int	Cob	Gama de color
	Conocimiento sobre el manejo y seguimiento a las redes sociales por parte de la institución con el fin de identificar	Reputación institucional	P.P	B	M	ALTO
	Posibles signos de vulnerabilidad entre estudiantes.	Datos y acceso credenciales	P	A	A	BAJO
	Conocimiento de casos donde la institución intervino por casos de vulnerabilidad en redes sociales.	Equipos informáticos	P.P	B	M	ALTO
	Promueve la institución el uso responsable y ético de las redes sociales.	Datos y acceso credenciales	P	A	A	BAJO
	Recursos para orientar a sus estudiantes en caso de presentar vulnerabilidad en redes sociales.	Reputación institucional	P	M	M	MEDIO
	Capacitaciones a estudiantes sobre la importancia de la privacidad y seguridad en línea.	Datos y acceso credenciales	M.P	A	A	BAJO
	Denuncias de vulnerabilidad en redes sociales con las autoridades escolares.					
	Educación sobre la seguridad en línea y protección de datos con los estudiantes.					

Tabla 18

Matriz de delitos informáticos en la institución

SITUACION	PROCESOS DE RIESGO	ACTIVOS AFECTADOS	CARACTERIZACIÓN			
			FR	INT	COB	GAMA DE COLOR
Delitos informáticos presentados en la institución educativa.	Conocimiento sobre delitos informáticos y vulnerabilidades en redes sociales.	Datos y acceso credenciales	P	A	A	BAJO
	Hackeos o suplantación de identidad en sus redes sociales.	Datos y acceso	P	M	M	MEDIO
	Infiltración de información en redes sociales.	Credenciales	P	M	A	ALTO

Tabla 19

Delitos informáticos con mayor incidencia.

Delito	Nivel de Riesgo
Suplantación de identidad	Alto
Hackeo	Alto
Ciberacoso	Alto

Después de realizar el análisis de nivel de riesgo con la metodología Magerit e ISO/IEC 27001 se puede concluir lo siguiente:

Los activos de hardware de la IEM Ciudad de Pasto, están expuestos a un nivel de riesgo alto, ya que no poseen un sistema de antivirus que pueda proteger los equipos de ataques informáticos, además los estudiantes no tienen un conocimiento claro del tipo de seguridad que se maneja dentro de la institución para las herramientas informáticas utilizadas en el desarrollo de las actividades educativas.

El nivel de riesgo de las amenazas presentadas en redes sociales para los integrantes de la comunidad educativa estudiada es medio, ya que, en áreas como contraseñas, protección de la información sensible, medidas de seguridad en perfiles la evaluación de riesgo es baja, pero en aspectos fundamentales como ataques de personas desconocidas, aumento del acoso estudiantil y exposición de datos personales, la evaluación de riesgo es alto, generando una exposición y riesgo de los estudiantes en este tipo de medios.

El nivel de riesgo para los casos de vulnerabilidad presentados dentro del plantel educativo es alto, ya que los estudiantes cuentan con poca información sobre la ruta de manejo que da la institución, no tienen un nivel de confianza alto en las áreas encargadas de la orientación escolar, la educación y la capacitación sobre cómo enfrentar un ataque cibernético es baja, exponiendo a

los miembros de la comunidad educativa a ser presas fáciles de los ataques y vulnerabilidad informáticas.

Aplicando La norma ISO/IEC 27001 la Institución Educativa Municipal (IEM) San Juan de Pasto responde a la necesidad crítica de garantizar la seguridad y protección de la información en un entorno digital cada vez más expuesto a riesgos y amenazas. Esta norma internacional proporciona un marco robusto y sistemático para la gestión de la seguridad de la información, lo que permite identificar, evaluar y mitigar las vulnerabilidades específicas que pueden comprometer la privacidad y seguridad de los datos en redes sociales.

La adopción de la ISO/IEC 27001 asegura que se establezcan políticas y controles efectivos para proteger la información sensible de los estudiantes, docentes y la comunidad educativa en general. Además, fomenta una cultura de seguridad en la institución, promoviendo la concienciación y la formación continua en buenas prácticas de ciberseguridad. Este enfoque no solo reduce la probabilidad de incidentes de seguridad, sino que también fortalece la capacidad de respuesta ante posibles brechas y ataques, minimizando su impacto y asegurando la continuidad de las operaciones educativas.

En resumen, la aplicación de la ISO/IEC 27001 en este proyecto es una decisión estratégica que refuerza la confianza en la gestión de la información de la IEM San Juan de Pasto, al mismo tiempo que protege los datos personales y garantiza el cumplimiento de las normativas legales y regulatorias. Este compromiso con la seguridad de la información no solo protege a la comunidad educativa, sino que también posiciona a la institución como un referente en la adopción de estándares internacionales de seguridad, promoviendo un entorno educativo seguro y resiliente frente a las amenazas cibernéticas.

2.4.2 Valoración de activos mediante la norma ISO/IEC 27001

Se realiza una evaluación cualitativa y cuantitativa de los activos de información

Valoración cualitativa

La valoración de los activos se realiza de acuerdo a su nivel de criticidad para la gestión institucional

Propiedades

Las siguientes propiedades se valoran para cada uno de los activos

Se evalúan las siguientes propiedades:

- Confidencialidad
- Integridad
- Disponibilidad
- Autenticidad

Para esta valoración se toma como referencia la siguiente escala:

- A = Alto
- M= Medio
- B = Bajo

Evaluación por propiedades

Tabla 20

Evaluación de activos por propiedades

No	Nombre del Activo de Información	Propiedades			
		Confidencialidad	Integridad	Disponibilidad	Autenticidad
1.	Equipos informáticos	M	M	A	B
2.	Servidores	M	M	A	B
3.	Software de gestión del aprendizaje (LMS)	M	M	M	M

4.	Red de área local (LAN)	M	M	M	M
5.	Recursos en la nube	M	M	M	B
7	Datos y acceso credenciales	A	A	MA	M
6	SAPRED	M	M	M	M
8	SIMAD	M	M	M	M
9	SECOD	M	M	M	M
10	SEM	M	M	M	M

Clasificación de activos de información

Marcando con una "X" se debe clasificar el activo de información si es físico o electrónico

Tabla 21

Clasificación de activos

No	Nombre del activo de información	Físico	Electrónico
1.	Equipos informáticos	X	
2.	Servidores	X	
3.	Software de gestión del aprendizaje (LMS)		X
4.	Red de área local (LAN	X	
5.	Recursos en la nube		X
6	Datos y acceso credenciales		X
7	SAPRED		X
8	SIMAD		X
9	SECOD		X
10	SEM		X

Valoración cuantitativa

La valoración cuantitativa está definida por la siguiente escala:

Tabla 22

Valoración de activos en la institución

	Nomenclatura	Categoría	Valoración
Valoración del riesgo	**MA**	**Crítico**	**21 a 25**
	A	**Importante**	**16 a 20**
	M	**Apreciable**	**10 a 15**
	B	**Bajo**	**5 a 9**
	MB	**Despreciable**	**1 a 4**

Basándose en la evaluación asignada a cada activo según los criterios establecidos en las cuatro dimensiones (ver tabla 20), la siguiente tabla se genera automáticamente.

Tabla 23

Propiedades de los activos

No	Nombre			Propiedades			
		Riesgo	Confidencialidad	Integridad	Disponibilidad	Autenticidad	VALOR
1.	Equipos informáticos	Apreciable	10	10	20	9	12
2.	Servidores	Apreciable	10	10	20	9	12
3.	Software de gestión del aprendizaje (LMS)	Apreciable	10	10	15	10	11
4.	Red de área local (LAN)	Apreciable	10	10	15	10	11
5.	Recursos en la nube	Apreciable	15	15	9	5	11
6	SAPRED	Apreciable	10	10	10	15	11
7	Datos y acceso credenciales	Importante	20	20	22	20	20
8	SIMAD	Apreciable	10	10	10	15	11
9	SECOD	Apreciable	10	10	10	15	11
10	SEM	Apreciable	10	10	10	15	11

A partir de la Tabla No 22 proporcionada, se puede deducir varias conclusiones sobre las propiedades y el valor de diferentes componentes tecnológicos en la Institución Educativa Municipal San Juan de Pasto:

Riesgo General: La mayoría de los componentes tecnológicos tienen un riesgo "Apreciable", con excepción de "Datos y acceso credenciales" que tiene un riesgo "Importante". Esto sugiere que, en términos generales, los componentes están en un nivel de riesgo medio, pero los datos y credenciales son considerados críticos y, por lo tanto, requieren mayor atención.

Confidencialidad, Integridad y Disponibilidad:

- La confidencialidad, integridad y disponibilidad son consistentemente calificadas con valores de 10 a 20 para todos los componentes. Los "Datos y acceso credenciales" tienen los valores más altos (20 en confidencialidad e integridad, y 22 en disponibilidad), destacando su importancia crítica en términos de seguridad.
- Otros componentes, como los "Recursos en la nube", tienen valores más bajos en disponibilidad (9), lo que podría indicar una necesidad de mejorar la disponibilidad de estos recursos.

Autenticidad:

- La autenticidad es más variable, con valores que van de 5 a 20. Nuevamente, "Datos y acceso credenciales" tienen el valor más alto (20), lo que indica su alta criticidad en términos de verificación de la autenticidad.
- Otros sistemas como "Recursos en la nube" tienen un valor relativamente bajo (5), sugiriendo un área potencial de mejora.

VALOR:

- El valor asignado a cada componente tecnológico varía entre 11 y 20. "Datos y acceso credenciales" tienen el valor más alto (20), destacando su relevancia extrema en el contexto educativo y de gestión.
- Otros componentes tienen valores de 11 o 12, indicando una importancia significativa pero no crítica.

Resumen de Conclusiones:

Mayor Prioridad: Los "Datos y acceso credenciales" son el componente más crítico, con el mayor riesgo y valor, y requieren medidas de seguridad rigurosas en las áreas (confidencialidad, integridad, disponibilidad y autenticidad).

- **Áreas de Mejora**: Los "Recursos en la nube" presentan una menor disponibilidad y autenticidad comparadas con otros componentes, sugiriendo áreas donde se pueden enfocar esfuerzos para mejorar la infraestructura y la seguridad.
- **Consistencia en Otros Componentes**: La mayoría de los otros componentes tecnológicos tienen valores y riesgos similares, lo que facilita la implementación de políticas de seguridad homogéneas para estos elementos.
- **Enfoque Integral**: Es esencial un enfoque integral para abordar tanto los componentes críticos como los apreciables, asegurando una estrategia de seguridad y gestión de riesgos equilibrada y eficaz para toda la institución.

Estas deducciones pueden ayudar a priorizar los recursos y esfuerzos en la implementación y mantenimiento de la norma ISO/IEC 27001 en la Institución Educativa Municipal San Juan de Pasto.

2.4.3 Identificación de amenazas en la institución

Se identifican amenazas que están dentro sobre cada activo. las amenazas definidas dentro de la metodología Magerit las cuales se resumen en la tabla 18

Tabla 24

Identificación de amenazas con Magerit.

Tipo De Amenaza	Amenaza
[E] Errores y fallos no intencionados	[E1] Vulnerabilidades de los programas (software)
[E] Errores y fallos no intencionados	[E2] Errores de mantenimiento / actualización de equipos (hardware)
[E] Errores y fallos no intencionados	[E3] Impacto en el rendimiento académico
[A] Ataques intencionados	[A1] Divulgación de información falsa o inapropiada

[A] Ataques intencionados	[A2] Acoso y ciberacoso
[E] Errores y fallos no intencionados	[E4] Manipulación de los equipos
[A] Ataques intencionados	[A3] Violación de la privacidad
[E] Errores y fallos no intencionados	[E5] Desconocimiento de ciberseguridad
[E] Errores y fallos no intencionados	[E6]Afectación de la imagen institucional

Fuente: Esta investigación

Como ya se ha señalado, la catalogación de los activos es de suma importancia, ya que esto determina la correcta relación entre el tipo de activo de información y las diversas amenazas en los grados decimo y once a las que puede estar expuesto. Después de este paso, se vinculan las amenazas con una o más vulnerabilidades, y luego se procede a definir el plan de tratamiento de riesgos, basado en el nivel de riesgo aceptable que se explicará más adelante.

2.4.4. Diseño del plan para gestionar riesgos mediante el uso de las directrices de calidad establecida en la norma ISO/IEC 27001

Existen cuatro opciones de tratamiento de riesgo:

- **Reducir el riesgo**: Implica la acción de reducir los posibles peligros a un nivel considerado aceptable, mediante la implementación de medidas de seguridad.
- **Transferir el riesgo:** La delegación de riesgos consiste en una táctica de administración y regulación de riesgos que supone la transferencia contractual de un riesgo determinado de una entidad a otra. Un caso típico es cuando se adquiere una póliza de seguro, mediante la cual se traslada un riesgo concreto de pérdida del titular de la póliza a la compañía aseguradora.
- **Evitar el riesgo:** La prevención de riesgos implica la anticipación y la eliminación de amenazas, actividades y exposiciones que puedan afectar adversamente los activos de información de una organización. A diferencia de la gestión de riesgos, cuyo propósito es mitigar los daños y las pérdidas financieras asociadas con eventos amenazantes, la prevención de riesgos tiene como objetivo evitar completamente la ocurrencia de dichos eventos."

- **Aceptación del riesgo:** implica reconocer y registrar el riesgo dentro del proceso de gestión de riesgos, pero no tomar ninguna medida preventiva. Se admite la posibilidad de que ocurra y se aplicará un plan específico solo si se materializa. Esta estrategia se recomienda para riesgos de magnitud insignificante, es decir, aquellos que no afectarán significativamente las operaciones de la organización si se materializan y para los cuales existe una solución sencilla si surge. Esta elección se justifica cuando el costo de implementar una estrategia alternativa para mitigar el riesgo supera los recursos necesarios para aceptar el riesgo.

2.5. Guía para la implementación de la ISO /IEC 27001 en la IEM San Juan de Pasto

La implementación de la norma ISO/IEC 27001 en instituciones educativas es un proceso fundamental para garantizar la calidad y seguridad de la información gestionada. En la Institución Educativa Municipal San Juan de Pasto, este desafío se convierte en una oportunidad para fortalecer su infraestructura tecnológica y administrativa. Esta guía se presenta como una herramienta clave para acompañar a la institución en cada paso del proceso, ofreciendo una visión detallada de los requisitos, procedimientos y beneficios que conlleva la adopción de la norma. A través de esta implementación, se busca no solo cumplir con estándares internacionales, sino también promover una cultura de mejora continua y eficiencia en la gestión educativa, asegurando un entorno seguro y de alta calidad para toda la comunidad educativa.

Política de seguridad de la información para la institución educativa municipal San Juan de Pasto

El Colegio Ciudad de Pasto reconoce la importancia crítica de proteger la confidencialidad, integridad y disponibilidad de la información por completo. La seguridad de la información es un componente fundamental de nuestra operación y una responsabilidad compartida por todos los miembros de la comunidad educativa. Esta política establece el marco general para la gestión de la seguridad de la información en el Colegio Ciudad de Pasto, basado en los principios y requisitos de la norma ISO/IEC 27001

Objetivos

- Defender la información confidencial de la institución educativa contra accesos no autorizados, modificaciones no deseadas, divulgaciones indebidas y destrucción accidental o malintencionada.
- Proteger los sistemas de información y los recursos tecnológicos contra amenazas internas y externas
- Asegurar la disponibilidad y la continuidad de los servicios de tecnología de la información críticos para las operaciones del colegio.
- Cumplir con las leyes regulaciones y requisitos contractuales relacionados con la seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, estudiantes y docentes en la institución educativa Municipal San Juan de Pasto.
- Buen manejo y uso de las redes sociales.

Alcance y aplicabilidad

Esta política se aplica a todos los aspectos relacionados con la gestión de la seguridad de la información en el Colegio Ciudad de Pasto, incluyendo:

- Sistemas de información y tecnología de la información
- Datos de estudiantes, padres, personal y administrativos.
- Procesos operativos y actividades relacionadas con la información.

Principios de seguridad de la información

- Confidencialidad: Garantiza la información confidencial se maneje y proteja adecuadamente para prevenir su divulgación no autorizada.
- Integridad: Mantener la precisión y la integridad de la información, evitando modificaciones no autorizadas o no deseadas.
- Disponibilidad: Asegura la información y los servicios estén disponibles cuando sean necesarios para el cumplimiento de las actividades educativas y administrativas.

- Cumplimiento de todas las leyes, regulaciones y normativas aplicables relacionadas con la seguridad de la información, así como con los requisitos contractuales relevantes.

Estrategias

La vulnerabilidad en plataformas virtuales y redes sociales es una preocupación importante para los estudiantes de educación media, ya que pueden enfrentar riesgos como el ciberacoso, el phishing, la exposición a contenido inapropiado y la violación de su privacidad. Estas estrategias podrán abordar y mitigar estas vulnerabilidades:

Estrategia 1: Educación y concientización

Talleres y seminarios

- Organizar talleres sobre ciberseguridad para educar a los estudiantes sobre cómo proteger su información personal y reconocer amenazas en línea.
- Uso Responsable de redes sociales: Realizar seminarios que enseñen el uso adecuado y seguro de las redes sociales, enfatizando la importancia de la privacidad y la etiqueta digital.

Material didáctico

- Guías y Manuales: Distribuir guías sobre cómo crear contraseñas seguras, configurar la privacidad en las redes sociales y evitar el phishing
- Videos Educativos: Producir o compartir vídeos que expliquen los riesgos en línea y cómo evitarlos.

Estrategia 2: Políticas y Normativas

Normativas Escolares

- Políticas de Uso de Internet: Establecer políticas claras sobre el uso de internet y las redes sociales en el entorno escolar, incluyendo sanciones por mal uso.

- Protección de Datos: Implementar políticas de protección de datos para asegurar que la información de los estudiantes esté resguardada.

Supervisión y Monitoreo

- Software de Monitoreo: Utilizar software que permita supervisar el uso de internet en dispositivos escolares para detectar actividades sospechosas o inapropiadas.
- Alertas Tempranas: Configurar sistemas de alertas tempranas que notifiquen a los administradores escolares sobre posibles incidentes de ciberacoso o amenazas en línea.

Estrategia 3: Habilidades Digitales

Desarrollo de Competencias

- Pensamiento Crítico: Fomentar el pensamiento crítico en la evaluación de la información en línea y las interacciones en redes sociales.
- Resolución de Problemas: Enseñar a los estudiantes cómo actuar si se encuentran en una situación comprometida en línea, incluyendo cómo reportar y bloquear usuarios.

Estrategia 4: Apoyo Psicológico y Emocional

Asesoramiento y Apoyo

- Consejería Escolar: Proveer servicios de consejería para apoyar a los estudiantes que han sido víctimas de ciberacoso o que se sienten vulnerables en línea.
- Programas de Resiliencia: Implementar programas que fortalezcan la resiliencia emocional y la autoestima de los estudiantes, ayudándolos a manejar el estrés y la presión social en las redes.

Intervención Temprana

- Detección de Problemas: Capacitar a maestros y personal escolar para detectar signos de ciberacoso o problemas emocionales relacionados con el uso de redes sociales.
- Redes de Apoyo: Crear redes de apoyo entre estudiantes para fomentar una cultura de respeto y apoyo mutuo en línea y fuera de línea.

Estrategia 5: Involucramiento de Padres y Comunidad

Participación de los Padres

- Talleres para Padres: Organizar talleres para educar a los padres sobre los riesgos en línea y cómo pueden ayudar a sus hijos a navegar de manera segura.
- Comunicación Abierta: Fomentar una comunicación abierta entre padres e hijos sobre el uso de internet y las experiencias en redes sociales.

Colaboración Comunitaria

- Alianzas con Expertos: Colaborar con expertos en ciberseguridad y organizaciones no gubernamentales para proporcionar recursos y apoyo adicional.
- Campañas de Sensibilización: Lanzar campañas comunitarias para sensibilizar sobre los riesgos en línea y promover un comportamiento seguro y responsable.

Estrategia 6: Uso de Tecnología Segura

Herramientas de Seguridad

- Software de Protección: Promover el uso de antivirus, firewalls y otros programas de seguridad en los dispositivos utilizados por los estudiantes.
- Actualizaciones Regulares: Asegurarse de que todos los dispositivos y software estén actualizados para proteger contra vulnerabilidades y amenazas.

Implementar estas estrategias puede ayudar a reducir las vulnerabilidades de los estudiantes en plataformas virtuales y redes sociales, creando un entorno más seguro y saludable para su desarrollo digital.

Responsabilidades

- La dirección del colegio es responsable de establecer un marco de gestión de la seguridad de la información, asignar recursos adecuados y promover una cultura de seguridad.
- El personal es responsable de cumplir con las políticas y procedimientos de seguridad de la información, así como de reportar cualquier incidente de seguridad que pueda surgir.
- El equipo de tecnología de la información es responsable de implementar y mantener controles de seguridad efectivos para proteger los sistemas y datos del colegio.

Gestión de riesgos

- Se Realizará evaluaciones periódicas de riesgos de seguridad de la información para identificar y mitigar posibles amenazas y vulnerabilidades
- Se implementará controles de seguridad adecuados para reducir los riesgos a un nivel aceptable y proteger los activos de información críticos.

Revisión y mejora

- Se revisará periódicamente el desempeño de los controles de seguridad de la información y realizamos mejoras según sea necesario.
- Mantener la política actualizada para reflejar los cambios en el entorno de seguridad de la información y los requisitos de la norma ISO/IEC 27001

Cumplimiento

Esta política de seguridad de la información es de obligado cumplimiento para todos los miembros del Colegio Ciudad de Pasto. El incumplimiento de esta política puede resultar en acciones disciplinarias, incluyendo la terminación del empleo o la expulsión de los estudiantes.

Esta política de seguridad de la información proporciona un marco sólido para proteger los activos de información del Colegio Ciudad de Pasto y promover una cultura de seguridad entre todos los miembros de la comunidad educativa.

2.5.1. Tabla de controles por dominios

Tabla 25

Controles de dominios de la norma ISO/IEC 2700

Controles de seguridad de la información de acuerdo a la norma ISO/IEC 27001 en la Institución educativa Municipal San Juan de Pasto.

Dominio	Subdominio	Control actual	Objetivos de control	Aplica	Justificación
A.5 Políticas de seguridad de la información	A.5.1. Orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.	A.5.1.1	Políticas de seguridad de la información	SI	Control: Se adopta este control, puesto que las políticas se deben revisar a intervalos planificados, o sí ocurren cambios significativos para asegurar su conveniencia. Adecuación y eficacias continuas.
		A.5.1.2	Revisión de las Políticas para la seguridad de la Información	SI	Se adopta este control, puesto que las políticas se deben revisar a intervalos planificados, o sí ocurren cambios significativos para asegurar su conveniencia. Adecuación y eficacias continuas.
A.6 Organización de la seguridad de la información	A.6.2 Dispositivos móviles y teletrabajo	A.6.2.1	Organización de la seguridad de la información	SI	Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A.7 Seguridad de los recursos humanos	A.7.2 Durante la ejecución del empleo	A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	NO	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.

Dominio	Subdominio	Control actual	Objetivos de control	Aplica	Justificación
		A.7.2.3	Proceso disciplinario	NO	Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
A.8 Gestión de activos	A.8.1 Responsabilidad por los activos	A.8.2.1	Clasificación de la información	NO	La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
A.9 Control de acceso	A.9.2 Gestión de acceso de usuarios	A.9.2.4	Gestión de información de autenticación secreta de usuarios	NO	La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.
	A.9.3 Responsabilidades de los usuarios	A.9.3.1	Uso de la información de autenticación secreta	NO	Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta
	A.9.4 Control de acceso a sistemas y aplicaciones	A.9.4.1	Restricción de acceso Información	SI	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.
		A.9.4.2	Procedimiento de ingreso seguro	SI	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.

Dominio	Subdominio	Control actual	Objetivos de control	Aplica	Justificación
		A.9.4.3	Sistema de gestión de contraseñas	NO	Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.
		A.9.4.4	Uso de programas utilitarios privilegiados	SI	Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.
A.11 Seguridad física y del entorno	A.11.1 Áreas seguras	A.11.1.4	Protección contra amenazas externas y ambientales	SI	Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
	A.11.2	A.11.2.4	Mantenimiento de equipos	SI	Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.
		A.11.2.7	Disposición segura o reutilización de equipos	NO	Control: Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.
		A.11.2.8	Equipos de usuario desatendidos	SI	Control: Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.

Dominio	Subdominio	Control actual	Objetivos de control	Aplica	Justificación
A.12 Seguridad de las operaciones	A.12.4 Registro y seguimiento	A.12.4.2	Protección de la información de registro	SI	Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.
	A.12.6 Gestión de la vulnerabilidad técnica	A.12.6.1	Gestión de las vulnerabilidades técnicas	NO	Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado
		A.12.6.2	Restricciones sobre la instalación de software	SI	Control: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.
	A.12.7 Consideraciones sobre auditorias de sistemas de información	A.12.7.1	Información controles de auditoría de sistemas	NO	Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
A.13 Seguridad de las comunicaciones	A.13.2 Transferencia de información	A.13.2.1	Políticas y procedimientos de transferencia de información	NO	Control: Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.
		A.13.2.2	Acuerdos sobre transferencia de información	NO	Control: Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.

Dominio	Subdominio	Control actual	Objetivos de control	Aplica	Justificación
		A.13.2.3	Mensajería electrónica	NO	Control: Se debería proteger adecuadamente la información incluida en la mensajería electrónica.
		A.13.2.4	Acuerdos de confidencialidad o de no divulgación	NO	Control: Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
A.14 Adquisición, desarrollo y mantenimientos de sistemas	A.14.1 Requisitos de seguridad de los sistemas de información	A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	NO	Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
		A.14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	NO	Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas
		A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	SI	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.

Dominio	Subdominio	Control actual	Objetivos de control	Aplica	Justificación
A.16 Gestión de incidentes de seguridad de la información	A.16.1 Gestión de incidentes y mejoras en la seguridad de la información	A.16.1.1	Responsabilidad y procedimientos	NO	Control: Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
		A.16.1.2	Reporte de eventos de seguridad de la información	SI	Control: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.
		A.16.1.3	Reporte de debilidades de seguridad de la información	SI	Control: Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
		A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	NO	Control: Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.
		A.16.1.5	Respuesta a incidentes de seguridad de la información	NO	Control: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados
		A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	NO	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.

Dominio	Subdominio	Control actual	Objetivos de control	Aplica	Justificación
		A.16.1.7	Recolección de evidencia	NO	Control: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio	A.17.1 Continuidad de seguridad de la información	A.17.1.1	Planificación de la continuidad de la seguridad de la información	SI	Control: La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
		A.17.1.2	Implementación de la continuidad de la seguridad de la información.	NO	Control: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
		A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	NO	Control: La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
	A.17.2 Redundancias	A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	NO	Control: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
A.18 Cumplimiento	A.18.1	A.18.1.3	Protección de registros	NO	Control: Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de

Dominio	Subdominio	Control actual	Objetivos de control	Aplica	Justificación
	Cumplimiento de requisitos legales y contractuales				acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
		A.18.1.4	Privacidad y protección de datos personales	NO	Control: Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.
	A.18.2 Revisiones de seguridad de la información	A.18.2.1	Revisión independiente de la seguridad de la información	NO	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
		A.18.2.2	Cumplimiento con las políticas y normas de seguridad	NO	Control: Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
		A.18.2.3	Revisión del cumplimiento técnico	SI	Control: Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

Conclusiones

La Institución Educativa Municipal Ciudad de Pasto cuenta con un sistema de gestión bien estructurado dividido en áreas directiva, académica, administrativa-financiera y comunitaria, cada una con procesos definidos para asegurar un funcionamiento eficiente y un ambiente educativo óptimo. El manejo de la información ha sido un pilar fundamental para la IEM, por lo que se hizo necesario evaluar las amenazas y vulnerabilidades que pudieran afectar su infraestructura tecnológica.

Encontramos que la I.E.M. Ciudad de Pasto posee una variedad de activos informáticos que incluyen equipos de hardware, software, redes de comunicación y datos, los cuales están catalogados y clasificados conforme al estándar ISO/IEC 27001. Esto permite una gestión adecuada de dichos activos, asegurando su protección y correcta utilización.

A través del análisis de riesgos basado en la metodología Magerit y la norma ISO/IEC 27001, se identificaron varias amenazas y vulnerabilidades más recurrentes en el proceso de evaluación se dio en las redes informáticas y en el uso de redes sociales por parte de los estudiantes. Entre estas amenazas se encuentran la falta de sistemas antivirus actualizados, el desconocimiento de medidas de seguridad y una alta exposición a ataques cibernéticos. La encuesta realizada a los estudiantes reveló que, aunque existe una conciencia general sobre los riesgos en redes sociales, hay una significativa falta de capacitación específica en ciberseguridad. Además, muchos estudiantes desconocen las políticas de seguridad y las rutas de manejo de incidentes dentro de la institución**.**

La valoración de los activos indicó que los datos y accesos credenciales son críticos y necesitan una protección robusta. Aunque otros activos no presentan un riesgo tan alto, también requieren medidas adecuadas de seguridad para garantizar la integridad y disponibilidad de la información.

La implementación de la norma ISO/IEC 27001 en el proyecto de vulnerabilidades en redes sociales de la IEM San Juan de Pasto responde a la necesidad de garantizar la seguridad y protección de la información en un entorno digital vulnerable a riesgos y amenazas. Esta norma proporciona un marco sistemático para la gestión de la seguridad de la información, permitiendo identificar, evaluar y mitigar las vulnerabilidades específicas. La adopción de la ISO/IEC 27001

establece políticas y controles efectivos, promueve la concienciación y la formación continua en ciberseguridad, y refuerza la confianza en la gestión de la información de la institución. Este compromiso no solo protege a la comunidad educativa, sino que también posiciona a la IEM como un referente en la adopción de estándares internacionales de seguridad, promoviendo un entorno educativo seguro y resiliente frente a las amenazas cibernéticas.

Recomendaciones

Se recomienda que la IEM Ciudad de Pasto divulgue el plan presentado, exponiendo las políticas, estrategias y acciones establecidas para mejorar la seguridad de la información. Esto garantizará que toda la comunidad educativa esté informada y comprometida con las medidas de seguridad. Asimismo, se propone que en la guía se incluya una tabla con estrategias, acciones, tiempos y responsables por cada estrategia, lo cual facilitará el seguimiento y la implementación efectiva de las medidas de seguridad.

Es fundamental mejorar la seguridad de los equipos informáticos mediante la instalación y el mantenimiento actualizado de sistemas de antivirus y otros programas de seguridad en todos los equipos de la institución. Además, se deben establecer políticas claras para la actualización regular de estos sistemas, asegurando que siempre estén protegidos contra las últimas amenazas.

Para fortalecer la ciberseguridad, se deben implementar programas de formación y talleres periódicos para estudiantes y personal, enfocándose en prácticas de ciberseguridad, el uso seguro de redes sociales y la identificación de amenazas en línea. Estos programas deben incluir la importancia de contraseñas seguras, la autenticación de dos factores y el manejo de información sensible.

Es crucial desarrollar y comunicar efectivamente las políticas de seguridad de la información a toda la comunidad educativa, asegurando que todos los miembros estén informados sobre los procedimientos a seguir en caso de incidentes de seguridad. Además, se debe continuar con la implementación de la norma ISO/IEC 27001 que le permita aplicar las políticas para fortalecer la seguridad de la información, lo cual incluye la gestión de riesgos, la evaluación de vulnerabilidades y la implementación de controles de seguridad de la institución.

Se debe mejorar la infraestructura de redes y equipos, asegurando que la infraestructura de red (LAN y servicios en la nube) esté configurada de manera segura y eficiente. También es importante proporcionar redundancia y medidas de respaldo adecuadas para garantizar la disponibilidad de los servicios.

Es esencial fomentar un ambiente de confianza en el cual los estudiantes se sientan seguros para reportar incidentes de ciberacoso o vulnerabilidad en redes sociales. Para ello, se deben establecer

canales de comunicación claros y seguros para la denuncia de estos casos. Además, se recomienda realizar auditorías y evaluaciones regulares de los sistemas de seguridad de la información para asegurarse de que las políticas y controles implementados sean efectivos, utilizando los resultados de estas evaluaciones para realizar mejoras continuas en el sistema de seguridad.

Implementar estas recomendaciones ayudará a la IEM Ciudad de Pasto a fortalecer su infraestructura de seguridad informática, proteger a sus estudiantes y personal de amenazas cibernéticas y asegurar un entorno educativo seguro y eficiente.

Referencias bibliográficas

Acosta, C (2021) Asuntos: legales, ciberseguridad subieron 37% durante el primer trimestre de 2020. 2021

Acosta, C (25 de enero de 2022) Conozca las sanciones por los ciberdelitos que más crecieron el año pasado. Asuntos Legales https:/asuntoslegales.com.co

Arias, D (2021) Ciberseguridad: uno de los retos que dejo el 2020.

Astorga, Schmidt (2019) Peligros de las redes sociales: cómo educar a nuestros hijos e hijas en ciberseguridad. Educare vol. 23 núm. 3

Ávila, R. (2013) Hacia una reflexión histórica de las TIC, Revista Hallazgos, vol. 10, núm. 19

Banco Interamericano de Desarrollo (2021) Reporte ciberseguridad 2020.

CISCO (2020) Defiéndase contra amenazas críticas de la actualidad, reporte de amenazas de 2019

Fernández, Hernández & Baptista (2012) Metodología de la investigación.

Forero, Nieto, Puerta, Valencia (2020) Investigación aplicada influencia del uso de redes sociales en los síntomas de ansiedad en jóvenes entre los 12 y los 18 años de edad en el colegio I.E María Cano.

Guzmán, C (2018) Seguridad aplicada en la utilización de redes sociales. Universidad Piloto de Colombia.

Millán, K (2018) Plataformas educativas. Universidad Nacional de Educación.

Pinto, A (2018) Funcionamiento familiar y adicción a las redes sociales en estudiantes de tercero, cuarto y quinto de secundaria.

Sampieri, R (2014) Metodología de la investigación, sexta edición.

Sánchez, R (2009) Plataformas de enseñanza virtual para entornos educativos.

Soler, A (2016) La confianza de los adolescentes escolarizados en las redes sociales virtuales. Praxis&Saber Vol.7 Núm. 15.

Romero, Figueroa, Vera, Álava, Morales (2018) Introducción a la seguridad informática y análisis de vulnerabilidades. Editorial área de innovación y desarrollo. UNESCO, (2020) Recursos Educativos Abiertos.

International Organization for Standardization (ISO). (2013). *ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements*.

ISO. Icontec (2022). GTC ISO/IEC 27001-27002, Guía técnica colombiana GTC ISO/IEC 2700127002.

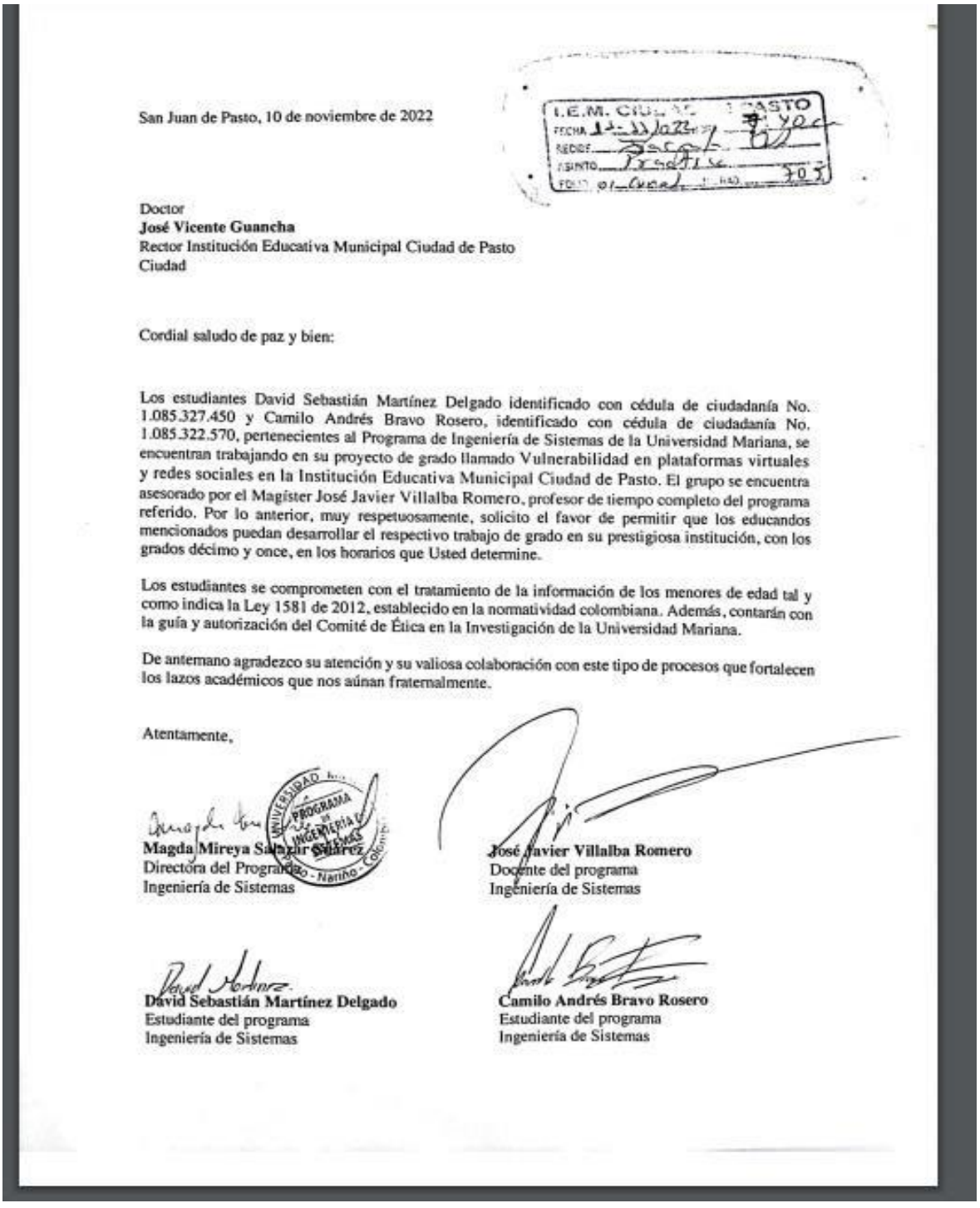
Institución Educativa Municipal Ciudad de Pasto. (2023). Diagrama de flujo de gestión Directiva. Recuperado de https://www.iemciudaddepasto.edu.co/gestion-directiva/.

Institución Educativa Municipal Ciudad de Pasto. (2023). Diagrama de flujo de gestión académica. Recuperado de https://www.iemciudaddepasto.edu.co/gestion-academica/.

Institución Educativa Municipal Ciudad de Pasto. (2023). Diagrama de flujo de gestión Administrativa y financiera. Recuperado de https://www.iemciudaddepasto.edu.co/gestionadministrativa-y-financiera/.

Institución Educativa Municipal Ciudad de Pasto. (2023). Diagrama de flujo de la gestión comunitaria. Recuperado de https://www.iemciudaddepasto.edu.co/gestion-comunitaria/.

Anexo 1 Aval de institucional



San Juan de Pasto, 10 de noviembre de 2022

I.E.M. CIUDAD DE PASTO
FECHA 14-11-2022
RADIF.
FOLIO

Doctor
José Vicente Guancha
Rector Institución Educativa Municipal Ciudad de Pasto
Ciudad

Cordial saludo de paz y bien:

Los estudiantes David Sebastián Martínez Delgado identificado con cédula de ciudadanía No. 1.085.327.450 y Camilo Andrés Bravo Rosero, identificado con cédula de ciudadanía No. 1.085.322.570, pertenecientes al Programa de Ingeniería de Sistemas de la Universidad Mariana, se encuentran trabajando en su proyecto de grado llamado Vulnerabilidad en plataformas virtuales y redes sociales en la Institución Educativa Municipal Ciudad de Pasto. El grupo se encuentra asesorado por el Magíster José Javier Villalba Romero, profesor de tiempo completo del programa referido. Por lo anterior, muy respetuosamente, solicito el favor de permitir que los educandos mencionados puedan desarrollar el respectivo trabajo de grado en su prestigiosa institución, con los grados décimo y once, en los horarios que Usted determine.

Los estudiantes se comprometen con el tratamiento de la información de los menores de edad tal y como indica la Ley 1581 de 2012, establecido en la normatividad colombiana. Además, contarán con la guía y autorización del Comité de Ética en la Investigación de la Universidad Mariana.

De antemano agradezco su atención y su valiosa colaboración con este tipo de procesos que fortalecen los lazos académicos que nos aúnan fraternalmente.

Atentamente,

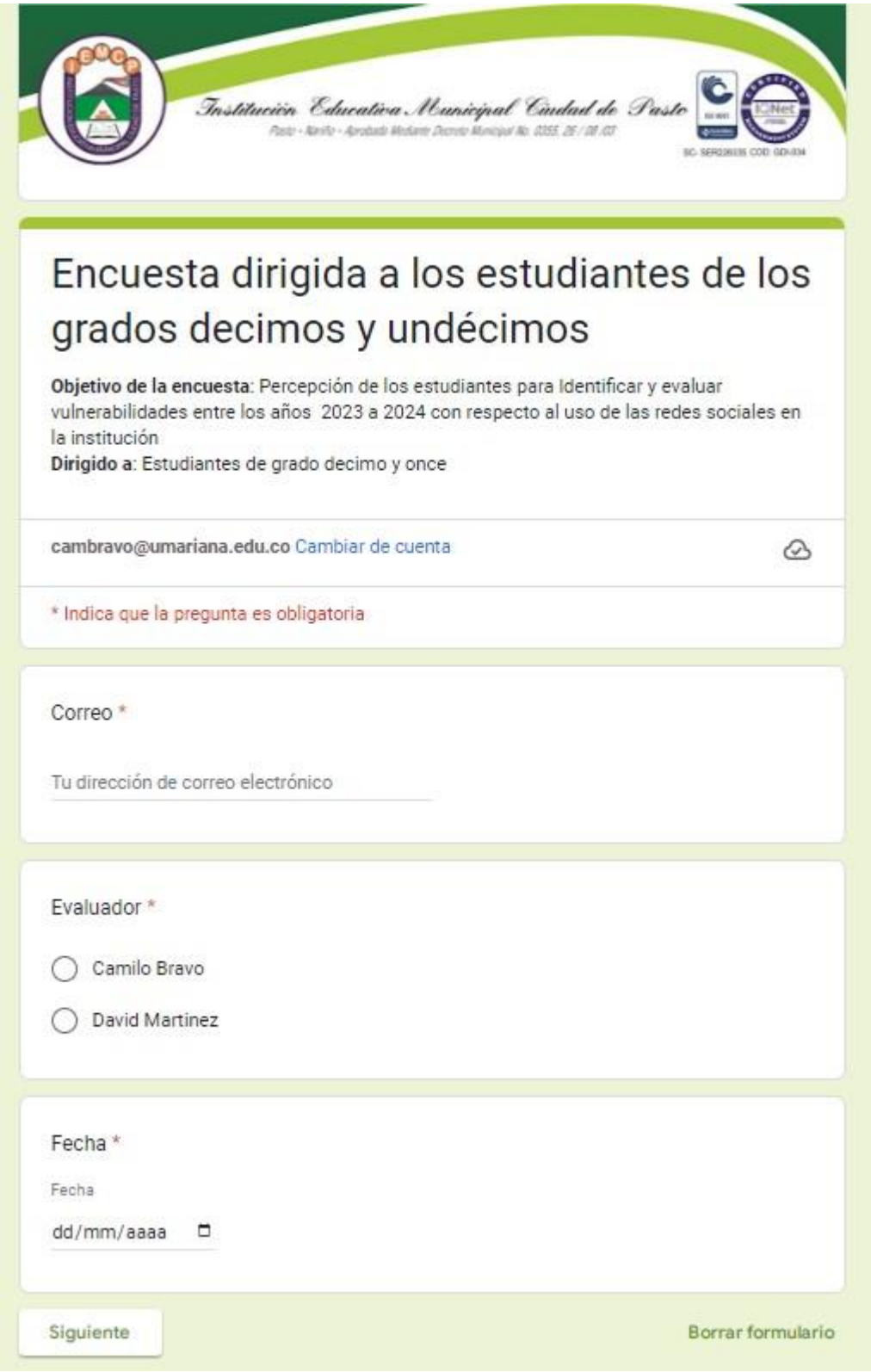
Magda Mireya Salazar Suárez
Directora del Programa
Ingeniería de Sistemas

José Javier Villalba Romero
Docente del programa
Ingeniería de Sistemas

David Sebastián Martínez Delgado
Estudiante del programa
Ingeniería de Sistemas

Camilo Andrés Bravo Rosero
Estudiante del programa
Ingeniería de Sistemas

Anexo 2 Formularios de encuesta



Encuesta dirigida a los estudiantes de los grados decimos y undécimos

cambravo@umariana.edu.co Cambiar de cuenta

* Indica que la pregunta es obligatoria

Aspectos generales

1) Grado: *

Elige

2) Edad: *

Elige

3) Género *

Elige

4) Rol *

◯ Estudiante

Aspectos específicos

5) ¿Qué dispositivos tecnológicos utiliza regularmente en sus actividades escolares o académicas ? *

- [ ] Equipos de computo
- [ ] Impresoras
- [ ] Tablet
- [ ] Celular
- [ ] Todos

6) ¿Con qué frecuencia utilizas las redes sociales? *

Elige

7) ¿Estás al tanto de las posibles amenazas y vulnerabilidades en las redes sociales? *

- ◯ Sí, estoy muy informado/a
- ◯ No, no estoy informado/a en absoluto

8) ¿Has experimentado alguna vez una vulnerabilidad o amenaza en tus perfiles de redes sociales? Por ejemplo, hackeo de cuenta, suplantación de identidad, acoso en línea, etc. *

- ◯ Si
- ◯ No

Atrás Siguiente Borrar formulario

Tipos de vulnerabilidad informática: ubícalos y protégete.

9) ¿En caso de que "SI" cual de los siguientes tipos de vulnerabilidades ha tenido ? *

- [ ] Hackeo
- [ ] Suplantación de identidad
- [ ] Trojans
- [ ] Complejidad de los sistemas
- [ ] Virus de redes sociales
- [ ] Impostores
- [ ] Infiltración de información
- [ ] Todas las anteriores
- [ ] Ninguna de las anteriores
- [ ] Otro: _____

10) ¿En las aulas de informática los equipos de computo poseen antivirus ? *

- ◯ Si
- ◯ No

11) ¿Si existen antivirus, las aulas de informática los equipos de computo estos antivirus están actualizados ? *

- ◯ Si
- ◯ No