GESTION DEL PROYECTO SOFTWARE DE ENSEÑANZA DE MATEMÁTICAS DE BACHILLERATO CON LA METODOLOGÍA MARCO LÓGICO Y MAGERIT 3.0

CURSO: PROYECTO DE INGENIERÍA II 202337121

PRESENTACIÓN DE RESULTADOS

GRUPO 88

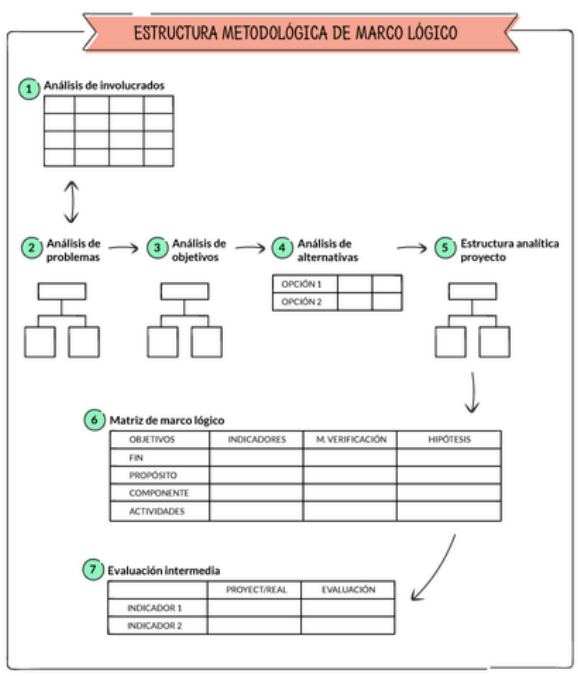
INTRODUCCIÓN

La gestión integral de un proyecto requiere un enfoque estructurado que permita definir el contexto de manera suficientemente clara, evitando omisiones o vacíos de factores involucrados, una buena visión general de la situación, posteriormente, plantear la ejecución mediante esquemas de actividades y la gestión de los riesgos. Pensando en ello, se aplican dos metodologías bien establecidas para este proyecto de desarrollo de software, que son el Marco Lógico y MAGERIT 3.0 para plantear las problemáticas, entorno y ejecución del proyecto, y para la gestión del riesgo, respectivamente.
La propuesta de proyecto es concretamente el desarrollo de software para educación en matemáticas a nivel de bachillerato.

De esta manera se intenta fortalecer el aprendizaje de esa ciencia básica, mediante el uso de tecnologías, que aporten valor al proceso.

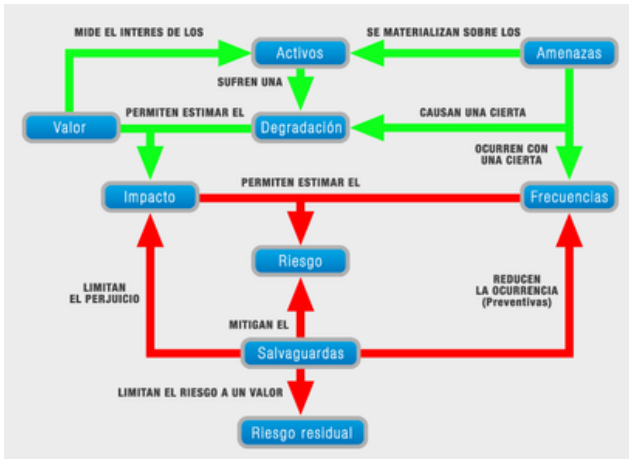
METODOLOGÍA

El **Marco Lógico** es una metodología de gestión de proyectos, enfocado a resultados y a partes interesadas. Ha sido perfeccionado, y con el tiempo ha incluido la definición de las partes interesadas, análisis del contexto, cronogramas de actividades y un esquema para monitorear y controlar la ejecución



Obtenido de:https://blog.ida.cl/estrategia-digital/metodologia-marco-logico-gestion-de-proyectos/

La metodología **MAGERIT 3.0** fue desarrollada por el gobierno español, para reducir los riesgos de la implantación y uso de las Tecnologías de la Información en contextos de gestión pública. Dada la disciplina en la que se implementa, será de utilidad para el proyecto de integración tecnológica de nuestra propuesta. Cuenta con una clasificación de componentes de uns proyecto, criterios de riesgos asociados, y el correspondiente tratamiento de estos.



Obtenido de: https://metodologiasderiesgo.blogspot.com/2014/12/analisis-de-riesgos.html

RESULTADOS

2 DESARROLLO DEL MARCO LÓGICO DEL PROYECTO DE SOFTWARE DIDÁCTICO PARA LA ENSEÑANZA DE MATEMÁTICAS DE SECUNDARIA

2.1 PLANTEAMIENTO DEL PROBLEMA:

En situaciones como la pandemia, u otras situaciones, en que la asistencia a clases de los niños se ve perjudicada, se pierde la continuidad educativa y los estudiantes no cuentan con una manera de continuar sus estudios de manera regular, y ordenada. Es muy oportuno contar con un producto digital que ofrezca flexibilidad y disponibilidad en entornos como el hogar, y que brinde la estructura y contenido de temas de matemáticas con interactividad llamativa y como complemento para ilustrar y mejorar la comprensión de nociones fundamentales de esta ciencia básica.

2.2 PROPUESTA IDEA DE DESARROLLO TECNOLÓGICO:

Desarrollar un software con cursos didácticos de matemáticas, preferiblemente de escritorio (Windows), que tengan distintos niveles de, por ejemplo, aritmética, álgebra, trigonometría e incluso una parte de cálculo diferencial. Con actividades interactivas, narradas, animadas gráficamente, y con quices que evalúen el nivel de entendimiento de los temas. Idealmente también, se podrían hacer serie de ejercicios con la misma finalidad de puntuar y evaluar el dominio de temas.

2.3 CLASIFICACIÓN DE LAS PARTES INTERESADAS

Parte Interesada	Interés / Rol dentro del proceso
Estudiantes	Realizar actividades que les resulten gratificantes, interesantes, útiles.
Padres de familia	Que sus hijos tengan buenos resultados en su aprendizaje, en sus puntuaciones académicas y puedan alcanzar mejores oportunidades en el futuro.
Docentes	Que su trabajo no se vea afectado por la herramienta, que sus sugerencias sean tenidas en cuenta en todo el proceso, poder contribuir en el desarrollo y tener un rol activo en el uso final.
Ministerio de educación	Hacer control a la validez del producto dentro de los planes de desarrollo del gobierno actual.
Organizaciones del sector público y privado	Las empresar desean emplear a trabajadores más calificados, que resuelvan mejor los retos de la operación de sus negocios y mejoren su competetitividad y rentabilidad.
Instituciones de educación secundaria, técnica y superior	Adaptación a este cambio, aprovechar sus características. Mejorar el prestigio de la institución. Ser tenidos en cuenta para las etapas del proceso
Sociedad en general	Mejores oportunidades laborales y de crecimiento profesional y personal.

Tabla 1. Involucrados y sus intereses

2.4 MATRIZ DE INFLUENCIA

En la matriz de influencia se valoran los aspectos de poder e interés que tiene cada actor identificado de la problemática para poder dar un tratamiento efectivo a esos factores y lograr un modelo del proyecto que satisfaga a los involucrados como usuarios u otros roles importantes del contexto.

Influencia	Bajo Interés	Alto Interés
Alta	**Mantener satisfechos** * Organizaciones publicas y privadas * * *	**Gestionar de cerca** * Ministerio de educación * Docentes * *
Baja	**Monitorear** * Sociedad en general * * *	**Mantener informados** * Estudiantes * Padres de familia * *

Tabla 2. Matriz de influencia

2.6 ANÁLISIS DE PROBLEMAS: ÁRBOL DE PROBLEMAS

Aplicando previamente la técnica de los cinco por qué, surgen aspectos esenciales como núcleos del problema, y se identifican una serie de problemas estructurales sociales, y las consecuencias de estas.

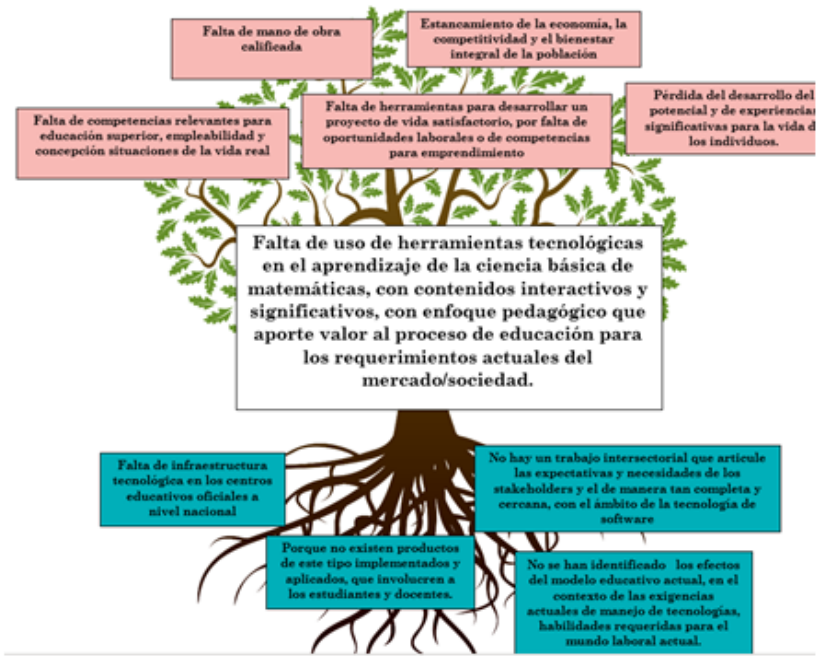


Figura 1. Árbol de problemas del caso del uso de tecnologías digitales en el modelo de educación.

2.7 JERARQUÍA DE OBJETIVOS

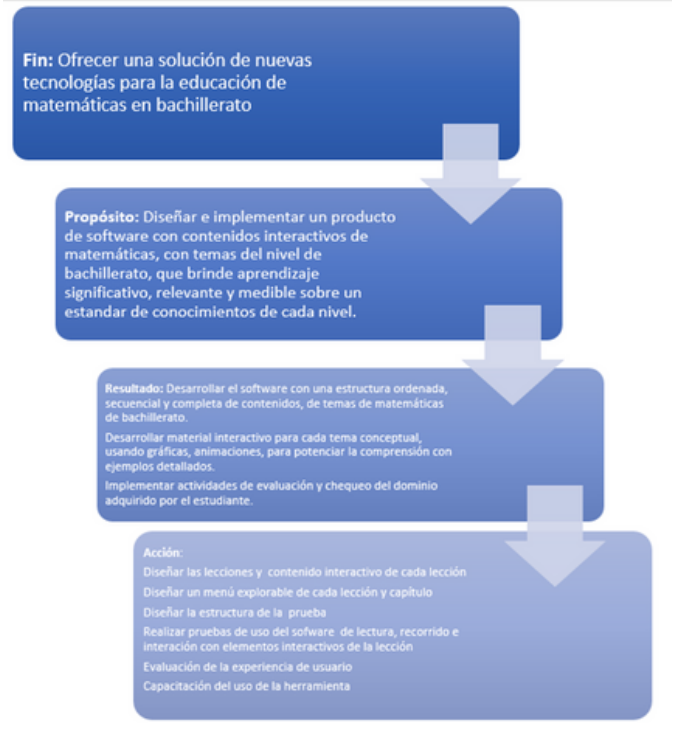


Figura 3. Jerarquía de objetivos del proyecto.

2.8 PRODUCTO MÍNIMO VIABLE

Para tener un punto de partida en la parte de ejecución es muy útil definir el producto mínimo viable.

¿Para quién?	Debe tener …	Debería tener…	Podría Tener…
Para niños(as) , adolescentes (as) y como material para docentes que llevan las clases de ellos(as).	• Contenidos gráficos, interactivos, multimedia, explicativos de cada tema. • Menú de contenidos, tipo índice. • Pruebas de dominio de cada tema.	• Guardado de progreso en el curso/ abrir la app en la página más reciente que se haya desarrollado del curso. • Un registro/promedio de las pruebas realizadas.	• Calculadora embebida • Tips para interactuar con el contenido y enfocar la atención en detalles gráficos, o coneptuales para entender un ejemplo. • Retroalimentación de evaluaciones. • Accesibilidad para personas con discpacidad auditiva.
Backlog Avisos visuales (mensajes desplegables) o de sonido para guiar en la manera de interactuar con el contenido interactivo, arrastrar el mouse, pinchar un botón, etc	**Alternativas** Tutoriales en video (youtube) Cursos online en plataformas como *edx, colombiaaprende, khanacademy*		

Figura 4. Propuesta del producto mínimo viable

2.9 ESTRUCTURA ANALÍTICA

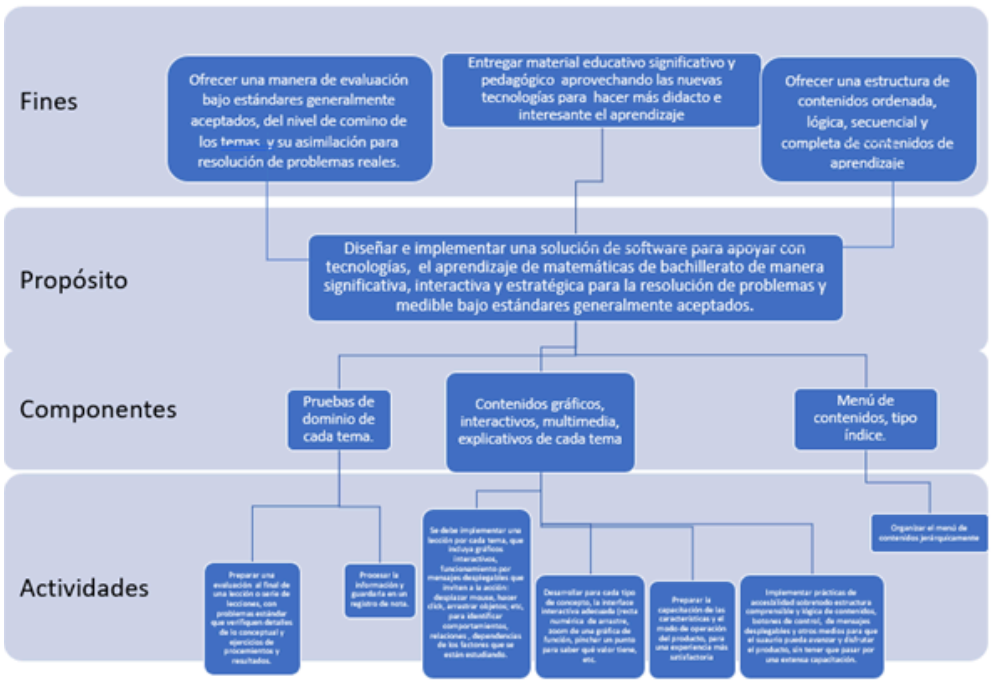


Figura 5. Estructura analítica del proyecto

3 MAGERIT : IDENTIFICACIÓN DE ACTIVOS

3.1 MATRIZ VALORACIÓN DE RIESGO:

En este paso, se identificaron principalmente activos tipo dato, en todo el código y archivos que requiere una aplicación de software de escritorio, se cuenta con hardware del computador de escritorio necesario para el uso del producto, un folleto que tiene las credenciales de instalación, que fue una característica que se decidió incluir, y de las personas directamente relacionadas; usuarios finales y desarrolladores. Las credenciales y datos de validación de credenciales tienen importancia en todas las dimensiones, ya que se plantea que el acceso sea autorizado y que el producto no se pueda usar sin control. En los atributos, de consideraron de impacto más grave, el acceso a datos de validación de credenciales, daños en el archivo ejecutable, que perjudica la funcionalidad del producto, y el conocimiento de los desarrolladores.

En la dimensión de confidencialidad, son críticos los activos de contraseñas, y código fuente del producto de software. En la dimensión de integridad, son críticos los activos de datos de configuración, código fuente, ejecutable y la cuestión de credenciales, que también ocupan un lugar crítico en la disponibilidad, ya que son esenciales para que el producto funcione.

Activos y Valoración Cualitativa

MATRIZ DE LEVANTAMIENTO DE INFORMACION DE ACTIVOS
SEGÚN METODOLOGIA MAGERIT Y NORMA ISO 27001:2013

Empresa: Ingeniería de Software- Tecnología para la educación. Fecha 16/4/20

INFORMACIÓN DE LOS ACTIVOS

No.	Nombre del activo de información	Proceso propietario del activo	Tipo de Activo	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Sistema expuesto en internet	Leve	Importante	Grave	Físico	Electrónico
2	Datos de configuración de la aplicación (carpeta de instalación, etc)		DATOS				MA	MA	NO	X				X
3	código fuente		DATOS			A	MA	M	NO		X			X
4	código ejecutable		DATOS				MA	MA	NO			X		X
5	registro de actividad		DATOS			B	M	M	NO	X				X
6	credenciales		DATOS	MA	MA	MA	MA	MA	NO		X			X
7	datos de validación de credenciales		DATOS	MA	MA	MA	MA	MA	NO			X		X
8	pc equipo de computo		HARDWARE					MA	SI		X		X	
9	material impreso con la clave del producto para ser instalado		SOPORTE	MA	MA	MA		MA	NO		X		X	
10	usuarios externos (finales)		PERSONAL		M				NO	X			X	
11	desarrolladores/programadores		PERSONAL		A	A			NO			X	X	
12														

Tabla 3. Análisis de

Fecha 16/4/2024

Sistema expuesto en internet	Leve	Importante	Grave	Físico	Electrónico	Descripción del Activo
NO	x				x	Estos datos serían básicamente los configurados por el usuario,y por defecto en la instalación
NO		x			x	El código en lenguaje de alto nivel, para escritorio C++, etc; que contiene el diseño del programa, las bibliotecas de funciones usadas,etc
NO			x		x	Este sería el código binario que el sistema operativo ejecuta directamente en el procesador, producto de la compilación
NO	x				x	Arhivos de puntajes guardados por el usuario en las evaluaciones con opción multiple, accesibles desde el software
NO		x			x	Son claves de acceso para la instalación del programa la primera vez
NO			x		x	Son datos en archivos, que sirven de referencia, para determinar la validez de las credenciales que el usuario ingresa.
SI		x		x		Recurso de hardware en el que se instala y ejecuta el software.
NO		x		x		Es una descripción del producto, e información de las credenciales asignadas para usar instalar y usar el producto(manual + licencia)
NO	x			x		el usuario académico, principalmente estudiantes, pero también docentes, que pueden reportar también errores, si los detectan a nivel de conteni
NO			x	x		son los diseñadores del producto, y responsables de la gestión de soporte durante su vida útil,

INF | METD | PYD | AVC | VC | APT

3.2 IDENTIFICACIÓN DE AMENAZAS

En dicho proceso se identificaron las amenazas contempladas en la metodología Magerit, V3.0 Sobre los activos que ya identificamos en el proyecto de “desarrollo de software didáctico para la enseñanza de matemáticas de secundaria”, que tiene su línea base en la Ingeniería de Software - tecnología para la educación.

Dichas amenazas se identificaron y se les dio una valoración la cual está tipificada en la metodología Magerit V3.0, la valoración que se le dio a dichas amenazas les asignamos de manera cuantitativa la cual tiene un rango dentro de la metodología teniendo en cuenta la probabilidad de ocurrencia con base en su posible frecuencia.

No. De Amenazas y Vulnerabilidades	Activos de información	Nombre del activo de información	Valoración del Riesgo de los Activos	Amenazas Metodologia Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración
1	DATOS	Ficheros de la interfaz gráfica del sistema operativo Windows	22	[E4] Errores de configuración	Descripción....	I	3
2	DATOS	Datos de configuración de la aplicación (carpeta de instalación, etc)	25	[E2] Errores del administrador		A	1
3	SOFTWARE	código fuente	20	[E8] Difusión de software dañino		A	2
4	SOFTWARE	código ejecutable	25	[E10] Errores de secuencia		A	1
5	CRIPTOGRAFICAS	registro de actividad	11	[A15] Modificación deliberada de la información		A	2
6	CRIPTOGRAFICAS	credenciales	25	[A11] Acceso no autorizado		A	1
7	DATOS	datos de validación de credenciales	25	[A5] Suplantación de la identidad del usuario		A	2
8	HARDWARE	pc equipo de computo	25	[I5] Avería de origen físico o lógico		A	1
9	DATOS	material impreso con la clave del producto para ser instalado	25	[E19] Fugas de información		A	2
10	PERSONAL	usuarios externos (finales)	15	[E28] Indisponibilidad del personal		A	2
11	PERSONAL	desarrolladores/programadores	20	[A6] Abuso de privilegios de acceso		A	1

Amenazas Metodologia Magerit
[E4] Errores de configuración
[E2] Errores del administrador
[E8] Difusión de software dañino
[E10] Errores de secuencia
[A15] Modificación deliberada de la información
[A11] Acceso no autorizado
[A5] Suplantación de la identidad del usuario
[I5] Avería de origen físico o lógico
[E19] Fugas de información
[E28] Indisponibilidad del personal
[A6] Abuso de privilegios de acceso

3.3 IDENTIFICACIÓN DE SALVAGUARDAS

Las salvaguardas se clasifican según el tipo de protección que ofrecen, como se identifica en la columna "Salvaguarda Tipo de Protección (Magerit)". Cada vulnerabilidad identificada en el sistema tiene asociada una salvaguarda que corresponde al tipo de protección necesaria para abordar esa vulnerabilidad específica.

Por ejemplo, para la vulnerabilidad de "Descargas de software desde fuentes no confiables o desconocidas", la salvaguarda propuesta es de tipo "Técnica", lo que implica que la medida de protección sugerida se basa en aspectos técnicos del sistema, como la implementación de políticas de control de acceso.

Salvaguarda Tipo de Protección (Magerit)	Acción a emprender	Riesgo residual	Criticidad residual
Organizativa	Implementar programas de capacitación en seguridad de la información de manera regular.	33	C
Tecnica	Establecer procedimientos de revisión por pares para verificar cambios en la configuración.	8	B
Tecnica	Implementar una política de control de acceso que restrinja las descargas de software a fuentes confiables y autorizadas.	40	C
Tecnica	Implementar procesos formales de desarrollo de software que incluyan pruebas de calidad y revisiones de código.	13	A
Tecnica	Implementar sistemas de control de acceso basados en roles que limiten el acceso a sistemas y bases de datos según las funciones y responsabilidades del usuario.	13	A
Tecnica	Configurar políticas de seguridad que requieran la autenticación multifactor para acceder a recursos sensibles.	13	A
Tecnica	Realizar pruebas de seguridad para asegurarse de que los métodos de autenticación implementados sean efectivos.	17	I
Tecnica	Establecer un programa de mantenimiento preventivo regular para sistemas y equipos críticos.	25	C
Tecnica	Implementar protocolos de cifrado robustos para proteger la confidencialidad de los datos en reposo y en tránsito.	25	C

CONCLUSIÓN Y DISCUSIÓN

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis at vestibulum ante. Nam id aliquet augue, et convallis quam. Nulla mauris odio, sagittis a lectus nec, imperdiet dignissim nunc. Aliquam condimentum lectus tristique, vehicula lectus eu, viverra diam. Nam congue diam non leo varius, vitae semper arcu

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis at vestibulum ante. Nam id aliquet augue, et convallis quam. Nulla mauris odio, sagittis a lectus nec, imperdiet dignissim nunc. Aliquam condimentum lectus tristique, vehicula lectus eu, viverra diam. Nam congue diam non leo varius, vitae semper arcu