



WWW.NEOBIO.COM
ASTURIAS

Neo**Biotech**
Technologies

2025



Objetivos

2025

1. DEFINIR EL PROYECTO Y SU TEMÁTICA ESPECÍFICA

Desarrollo:

El proyecto se centra en la creación de una plataforma web que permita a los usuarios detectar deepfakes (imágenes, videos o audios manipulados mediante inteligencia artificial). La temática específica es la ciberseguridad, con un enfoque en la protección contra la desinformación y el fraude digital causado por los deepfakes.

- Temática Principal: Ciberseguridad y protección contra deepfakes.
- Público Objetivo:
 - Usuarios individuales: Personas que quieran verificar la autenticidad de contenido multimedia.
 - Empresas y organizaciones: Entidades que necesiten proteger su reputación y verificar la autenticidad de contenido en sus plataformas.
- Valor Añadido: La plataforma no solo detectará deepfakes, sino que también educará a los usuarios sobre cómo identificar y protegerse contra este tipo de amenazas.



2025

2. ELABORAR LA DOCUMENTACIÓN INICIAL CON PLANIFICACIÓN, ESTUDIO DE ALTERNATIVAS Y ANÁLISIS DE REQUISITOS.

Desarrollo:

La documentación inicial incluirá:

- Planificación:
 - Diagrama de Gantt: Para visualizar las fases del proyecto y las tareas principales.
 - Cronograma: Establecer plazos para cada fase (documentación, desarrollo, pruebas, lanzamiento).
- Estudio de Alternativas:
 - Análisis de herramientas existentes (Deepware Scanner, Sensity AI, WeVerify).
 - Identificación de fortalezas y debilidades de la competencia.
 - Definición de cómo nuestra plataforma se diferenciará (interfaz intuitiva, recursos educativos, etc.).
- Análisis de Requisitos:
 - Requisitos Funcionales: Qué debe hacer la plataforma (subir archivos, analizar, mostrar resultados).
 - Requisitos No Funcionales: Rendimiento, usabilidad, compatibilidad con dispositivos móviles.
 - Diagrama de Casos de Uso: Para visualizar las interacciones de los usuarios con la plataforma.



2025

3. CONFIGURAR EL ENTORNO DE DESARROLLO Y CREAR UN REPOSITORIO EN GITHUB

Desarrollo:

Para garantizar un desarrollo organizado y colaborativo, es esencial configurar el entorno de desarrollo y utilizar un sistema de control de versiones como GitHub.

- Configuración del Entorno de Desarrollo:
 - IDE: Visual Studio Code .
 - Navegadores: Chrome y Firefox para pruebas.
 - Herramientas Adicionales: SQL, Git para control de versiones.
- Creación del Repositorio en GitHub:
 - Crear un repositorio público o privado para el proyecto.
 - Establecer una estructura de carpetas básica (por ejemplo, src para el código fuente, docs para la documentación).
 - Configurar un flujo de trabajo con Git (ramas para desarrollo, pruebas y producción).
- Integración Continua (CI): Configurar GitHub para automatizar pruebas y despliegues.



2025

4. DESARROLLAR LOS PRIMEROS PROTOTIPOS EN HTML, CSS Y JAVASCRIPT.

Desarrollo:

El desarrollo de prototipos es una fase clave para visualizar cómo será la plataforma y realizar ajustes antes de la implementación completa.

- Wireframes o Bocetos:
 - Página de Inicio: Bienvenida a la plataforma, botón para subir archivos.
 - Página de Análisis: Resultados del análisis de deepfakes.
 - Página Educativa: Tutoriales y artículos sobre ciberseguridad.
- Maquetación Inicial:
 - HTML: Estructura básica de la página web.
 - CSS: Estilos para mejorar la apariencia y usabilidad.
 - JavaScript: Funcionalidad básica para subir archivos y mostrar resultados.



2025

Introducción & Objetivos.

1. Introducción

Descripción del Proyecto:

El proyecto consiste en el desarrollo de una plataforma web dedicada a la protección contra deepfakes. Los deepfakes son videos, imágenes o audios manipulados mediante técnicas de inteligencia artificial (IA) que pueden ser utilizados para difundir desinformación, cometer fraudes o dañar la reputación de personas y organizaciones. Esta plataforma tiene como objetivo principal proporcionar herramientas y recursos para que los usuarios puedan detectar y protegerse contra este tipo de amenazas digitales.

Problemática a Resolver:

En la era digital, los deepfakes se han convertido en una amenaza creciente debido a su capacidad para engañar a las personas y manipular la información. Esto puede tener consecuencias graves, como:

Desinformación: Difusión de noticias falsas o manipuladas.

Fraude: Uso de deepfakes para suplantar identidades y cometer estafas.

Daño a la reputación: Creación de contenido falso que perjudica a personas o empresas.

La falta de herramientas accesibles y efectivas para detectar deepfakes hace que sea difícil para los usuarios comunes identificar contenido manipulado. Por lo tanto, este proyecto busca llenar ese vacío proporcionando una solución integral que combine tecnología de detección con educación y concienciación.



2025

2. Objetivos

Objetivo General:

Desarrollar una plataforma web que permita a los usuarios detectar deepfakes en imágenes, videos y audios, y que además proporcione recursos educativos para ayudar a los usuarios a comprender y protegerse contra este tipo de amenazas.

Objetivos Específicos:

1. Implementar una herramienta de detección de deepfakes:

- Crear un sistema que permita a los usuarios subir archivos multimedia (imágenes, videos, audios) para su análisis.
- Utilizar algoritmos de inteligencia artificial para detectar posibles manipulaciones en los archivos subidos.
- Proporcionar un informe detallado que indique si el archivo es auténtico o ha sido manipulado.

2. Desarrollar una sección educativa:

- Crear contenido educativo sobre qué son los deepfakes, cómo funcionan y por qué son una amenaza.
- Proporcionar guías y tutoriales sobre cómo identificar contenido manipulado.
- Ofrecer consejos prácticos para protegerse contra los deepfakes.

3. Diseñar una interfaz intuitiva y accesible:

- Desarrollar una interfaz de usuario sencilla y fácil de usar, accesible para usuarios de todos los niveles.
- Asegurar que la plataforma sea compatible con dispositivos móviles y diferentes navegadores.

4. Promover la concienciación sobre los deepfakes:

- Crear campañas de concienciación sobre los riesgos asociados con los deepfakes.
- Colaborar con organizaciones y medios de comunicación para difundir información sobre cómo detectar y prevenir este tipo de amenazas.



2025

La creciente sofisticación de las técnicas de manipulación de contenido multimedia ha hecho que los deepfakes sean una amenaza real y tangible. Aunque existen algunas herramientas y soluciones para detectar deepfakes, muchas de ellas son complejas o inaccesibles para el usuario promedio. Este proyecto busca democratizar el acceso a la tecnología de detección de deepfakes, proporcionando una plataforma fácil de usar y gratuita para todos.

Además, la educación es un componente clave en la lucha contra los deepfakes. Muchas personas no son conscientes de los riesgos asociados con este tipo de contenido manipulado. Por lo tanto, este proyecto no solo se enfoca en la detección técnica, sino también en la concienciación y educación de los usuarios.

Alcance del Proyecto

El proyecto se centrará en:

- Desarrollar una herramienta de detección de deepfakes basada en algoritmos de inteligencia artificial.
- Crear una sección educativa con recursos y tutoriales sobre cómo identificar y protegerse contra los deepfakes.
- Diseñar una interfaz de usuario intuitiva y accesible.
- Proporcionar soporte para imágenes, videos y audios como tipos de archivo para análisis.



Estudio de alternativas.

2025

El objetivo de este estudio es analizar las herramientas y plataformas existentes que abordan el problema de los deepfakes. Esto nos permitirá:

- Identificar las fortalezas y debilidades de las soluciones actuales.
- Determinar cómo nuestro proyecto puede diferenciarse y ofrecer un valor único.
- Aprender de las mejores prácticas y evitar los errores comunes.

Análisis de Alternativas Existentes.

A continuación, se presenta un análisis de algunas de las herramientas y plataformas más relevantes en el ámbito de la detección de deepfakes:

1. Deepware Scanner

Descripción: Deepware Scanner es una herramienta en línea que permite a los usuarios subir videos para detectar posibles deepfakes.

Fortalezas:

- Interfaz sencilla y fácil de usar.
- Proporciona resultados rápidos.
- Gratuita para uso básico.

Debilidades:

- Limitada a videos (no soporta imágenes o audios).
- No ofrece recursos educativos o de concienciación.
- La precisión de la detección puede variar.



2025

2. Sensity AI

- Descripción: Sensity AI es una plataforma que ofrece servicios de detección de deepfakes para empresas y organizaciones.
- Fortalezas:
 - Alta precisión en la detección de deepfakes.
 - Ofrece soluciones personalizadas para empresas.
 - Integración con sistemas de seguridad existentes.
- Debilidades:
 - No está dirigida a usuarios individuales.
 - Coste elevado para pequeñas empresas o particulares.
 - Falta de recursos educativos para el público general.

3. WeVerify

- Descripción: WeVerify es un proyecto europeo que combina inteligencia artificial y verificación humana para detectar contenido falso, incluyendo deepfakes.
- Fortalezas:
 - Enfoque en la verificación de noticias y contenido multimedia.
 - Combina tecnología automatizada con revisión humana.
 - Proyecto de código abierto.
- Debilidades:
 - No es una herramienta de uso directo para el público general.
 - Requiere conocimientos técnicos para su implementación.
 - No ofrece una interfaz amigable para usuarios no técnicos.



2025

Planificación del proyecto.

Objetivo de la Planificación.

El objetivo de esta sección es establecer un plan detallado que guíe el desarrollo del proyecto, asegurando que todas las tareas se completen y que los recursos se utilicen de manera eficiente. La planificación incluirá:

1. Un diagrama de Gantt para visualizar las tareas y plazos.
2. Las fases del proyecto y las tareas principales asociadas a cada fase.
3. Los recursos necesarios .

Fases del Proyecto.

El proyecto se dividirá en 4 fases principales, cada una con sus respectivas tareas y plazos:

Fase 1: Documentación y Prototipos (X semanas)

- **Objetivo:** Definir el proyecto, elaborar la documentación inicial y desarrollar los primeros prototipos.
- **Tareas Principales:**
 - a. Definición del proyecto:
 - Establecer los objetivos generales y específicos.
 - Realizar un estudio de alternativas y análisis de requisitos.
 - b. Documentación inicial:
 - Crear un documento de planificación con el alcance, los requisitos y el cronograma.
 - Desarrollar un diagrama de Gantt.
 - c. Configuración del entorno de desarrollo:
 - Configurar el IDE (Visual Studio Code), GitHub y otras herramientas necesarias.
 - d. Desarrollo de prototipos:
 - Crear wireframes o bocetos de la interfaz de usuario.
 - Desarrollar la maquetación inicial en HTML y CSS.
 - Implementar la funcionalidad básica en JavaScript.



2025

Fase 2: Desarrollo de la Plataforma (X semanas)

- Objetivo: Desarrollar la plataforma web con todas las funcionalidades principales.
- Tareas Principales:
 - a. Herramienta de detección de deepfakes:
 - Implementar el sistema de subida y análisis de archivos multimedia.
 - Integrar algoritmos de detección de deepfakes (usando modelos preentrenados o APIs externas).
 - b. Sección educativa:
 - Crear contenido educativo (tutoriales, artículos, guías).
 - Diseñar la interfaz para la sección educativa.
 - c. Diseño de la interfaz de usuario:
 - Desarrollar una interfaz intuitiva y accesible.
 - Asegurar la compatibilidad con dispositivos móviles y diferentes navegadores.
 - d. Integración de APIs:
 - Desarrollar una API para la detección de deepfakes (opcional, si se requiere integración con otros sistemas).

◦

Fase 3: Pruebas y Ajustes (X semanas)

- Objetivo: Realizar pruebas de usabilidad y rendimiento, y realizar los ajustes necesarios.
- Tareas Principales:
 - a. Pruebas de usabilidad:
 - Realizar pruebas con usuarios reales para evaluar la facilidad de uso de la plataforma.
 - Recopilar feedback y realizar ajustes en la interfaz y funcionalidades.
 - b. Pruebas de rendimiento:
 - Asegurar que la plataforma funcione correctamente en diferentes navegadores y dispositivos.
 - Optimizar el tiempo de respuesta del sistema.
 - c. Corrección de errores:
 - Identificar y corregir errores o bugs en el código.
 - d. Optimización:
 - Mejorar el rendimiento del sistema y la experiencia del usuario.



2025

Requisitos del sistema

4. REQUISITOS DEL SISTEMA

Los requisitos del sistema se dividen en requisitos funcionales (qué debe hacer el sistema) y requisitos no funcionales (cómo debe hacerlo). A continuación, se detallan ambos tipos:

4.1 Requisitos Funcionales.

Estos describen las funcionalidades que el sistema debe ofrecer para garantizar la ciberseguridad.

- Autenticación de usuarios:

El sistema debe permitir la autenticación de usuarios mediante credenciales (usuario y contraseña).

Debe implementar autenticación de dos factores (2FA) para acceder a áreas críticas.

- Control de acceso:

El sistema debe gestionar roles y permisos (administrador, usuario estándar, invitado).

Debe restringir el acceso a recursos sensibles según el perfil del usuario.

- Protección de datos:

El sistema debe cifrar datos sensibles (por ejemplo, contraseñas, información personal) tanto en tránsito como en reposo.

Debe implementar protocolos seguros como HTTPS y TLS.

- Registro y auditoría:

El sistema debe generar logs de actividades (logs de acceso, intentos fallidos, cambios en la configuración).

Debe permitir la auditoría de estos logs para identificar posibles brechas de seguridad.



2025

- Gestión de vulnerabilidades:

El sistema debe realizar escaneos periódicos para detectar vulnerabilidades.

Debe permitir la actualización automática de parches de seguridad.

- Copia de seguridad y recuperación:

El sistema debe realizar copias de seguridad periódicas de los datos críticos.

Debe contar con un plan de recuperación ante desastres (DRP).

- Protección contra malware:

El sistema debe incluir un antivirus y antimalware para detectar y eliminar amenazas.

Debe escanear archivos subidos por los usuarios.

4.2 REQUISITOS NO FUNCIONALES

Estos describen las características generales del sistema y cómo debe comportarse:

- Rendimiento:

El sistema debe manejar un mínimo de 1,000 usuarios concurrentes sin degradación del rendimiento.

El tiempo de respuesta para las operaciones críticas no debe superar los 2 segundos.

- Escalabilidad:

El sistema debe ser escalable horizontalmente para soportar un crecimiento en el número de usuarios y recursos.

- Disponibilidad:

El sistema debe garantizar una disponibilidad del 99.9% (alta disponibilidad).

Debe incluir redundancia de servidores y平衡adores de carga.



2025

- Seguridad:

El sistema debe cumplir con estándares de seguridad como ISO 27001, GDPR (si aplica) y OWASP Top 10.
Debe realizar pruebas de penetración periódicas.

- Usabilidad:

La interfaz de usuario debe ser intuitiva y fácil de usar, incluso para usuarios no técnicos.
Debe incluir documentación clara para administradores y usuarios finales.

- Compatibilidad:

El sistema debe ser compatible con los principales navegadores web (Chrome, Firefox, Safari, Edge).
Debe funcionar en sistemas operativos Windows, Linux y macOS.

- Mantenibilidad:

El código debe estar bien documentado y seguir buenas prácticas de desarrollo.
Debe permitir la implementación de actualizaciones sin interrupciones significativas.

- Cumplimiento legal:

El sistema debe cumplir con las normativas locales e internacionales de protección de datos (por ejemplo, GDPR en Europa o CCPA en California).



2025

4.3 REQUISITOS DE HARDWARE Y SOFTWARE

- Hardware:

Servidores con capacidad de procesamiento y almacenamiento suficiente para soportar la carga esperada.

Dispositivos de red seguros (firewalls, routers con cifrado).

- Software:

Sistemas operativos actualizados y parcheados.

Herramientas de seguridad como antivirus, IDS/IPS, y sistemas de gestión de logs.

4.4 REQUISITOS DE SEGURIDAD ADICIONALES

- Políticas de seguridad:

El sistema debe incluir políticas de contraseñas seguras (longitud mínima, complejidad, caducidad).

Debe implementar bloqueo de cuentas tras varios intentos fallidos de acceso.

- Privacidad:

El sistema debe garantizar la privacidad de los usuarios y cumplir con las normativas de protección de datos.

Debe incluir un aviso de cookies y políticas de privacidad claras.



Tecnologías



HTML



- Front-end: HTML5, CSS3 para la estructura y diseño.
- Back-end: Java para la lógica de negocio y funcionalidades interactivas.
- Base de datos (opcional): SQL si se requiere almacenamiento de casos de estudio o reportes.
- Seguridad: Implementación de HTTPS y protección contra ataques XSS.



Metodología de desarrollo

Se utilizará una metodología ágil, basada en la implementación iterativa de funcionalidades, con revisiones periódicas para garantizar que la plataforma sea intuitiva, eficaz y segura.

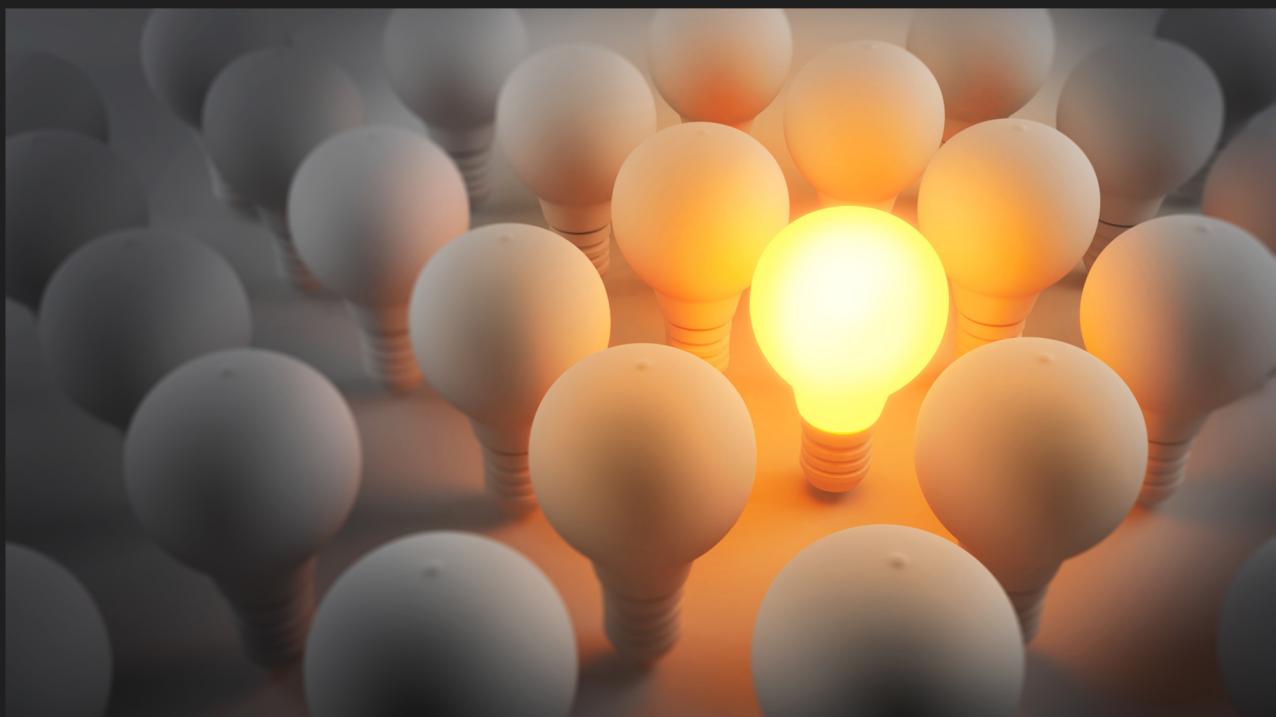


Fases de Desarrollo:

- Investigación y recopilación de información.
- Diseño de la estructura y wireframes del sitio.
- Desarrollo del front-end y back-end.
- Integración de herramientas interactivas.
- Pruebas y optimización.
- Despliegue y mantenimiento continuo.



Conclusión



Este proyecto busca ser una referencia en la lucha contra los deepfakes, proporcionando información clave y herramientas útiles para proteger la identidad digital de figuras públicas. La combinación de tecnología, educación y marcos legales permitirá crear una plataforma única y necesaria en la actualidad.